Proxy Server

Proxy Server adalah protokol yang digunakan untuk menjembatani koneksi internet dari klien ke server, dengan menggunakan proxy maka secara tidak langsung klien dipaksa mengikuti semua aturan yang sudah ditetapkan proxy. Beberapa aturan yang bisa ditetepkan meliputi hak akses, filtering conten, limiter download dan authentikasi password.

Squid adalah salah satu piranti lunak yang digunakan untuk menerapkan beberapa rule tersebut. Beberapa fitur yang dimiki squid meliputi beberapa fungsi parameter untuk meningkatkan kinerja dan optimasi secara maksimal tidak penulis jelaskan di buku ini, sebab secara teknik ukuran dalam kinerja squid berbeda-beda dari setiap individu.

Beberapa persiapan yang perlu diperhatikan dalam membangun squid adalah cache. Cache merupakan media penyimpanan khusus untuk menampung cache aktifitas browsing, sehingga cache sendiri perlu dikelompokkan dalam partisi sendiri, misalnya sebuah server dengan Harddisk ukuran 40GB akan dibagi menjadi beberapa partisi yaitu sebagai sistem utama, swap sebagai cadangan memori dan cache sebagai penyimpanan cache browsing, maka anda bisa membuatnya seperti ini :

1. Membuat partisi root (/) kapasitas harddisk 15 GB
2. Membuat partisi swap kapasitas harddisk 4 GB atau 2 kali besar memori
3. Membuat 3 partisi masing-masing 4 GB dengan direktori /cache01, /cache02 dan /cache03

Cara membuat partisi dengan metode penambahan partisi cache bisa anda lihat di bab yang menjelaskan installasi pada buku ini.

9.1. Installasi Squid

Selanjutnya jika persiapan tersebut sudah siap maka anda bisa memulai proses installasi proxy server menggunakan squid yaitu dengan menjalankan perintah dibawah ini :

```
[root@proxy ~]# yum install squid
```

Ketika proses installasi squid membutuhkan waktu sekitar 5 menit untuk download paket, jika proses installasi sudah selesai, silahkan membuka editor file utama squid.conf dengan perintah dibawah ini

```
[root@proxy ~]# vim /etc/squid/squid.conf
```

Cari baris 572 dan tambahkan alamat network anda seperti dibawah ini

```
acl my-network src 192.168.10.0/24
#Recommended minimum configuration:
```

Baris 628 tambahkan rule http_access seperti contoh berikut

```
http_access allow my-network
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
```

Baris 3008 tambahkan nama hostname yang digunakan, penulis menggunakan proxy.centos.co.id

```
visible_hostname proxy.centos.co.id
```

Baris 4280 setting menjadi OFF berfungsi menyembunyikan IP Address

```
forwarded_for off
```

Konfigurasi tersebut merupakan beberapa parameter standart yang digunakan proxy server, jika sudah selesai simpan konfigurasi anda dan restart service squid

```
[root@proxy ~]# service squid restart
Stopping squid: ..............                             [  OK  ]
Starting squid: .                                          [  OK  ]
[root@proxy ~]#
[root@proxy ~]# chkconfig squid on
```

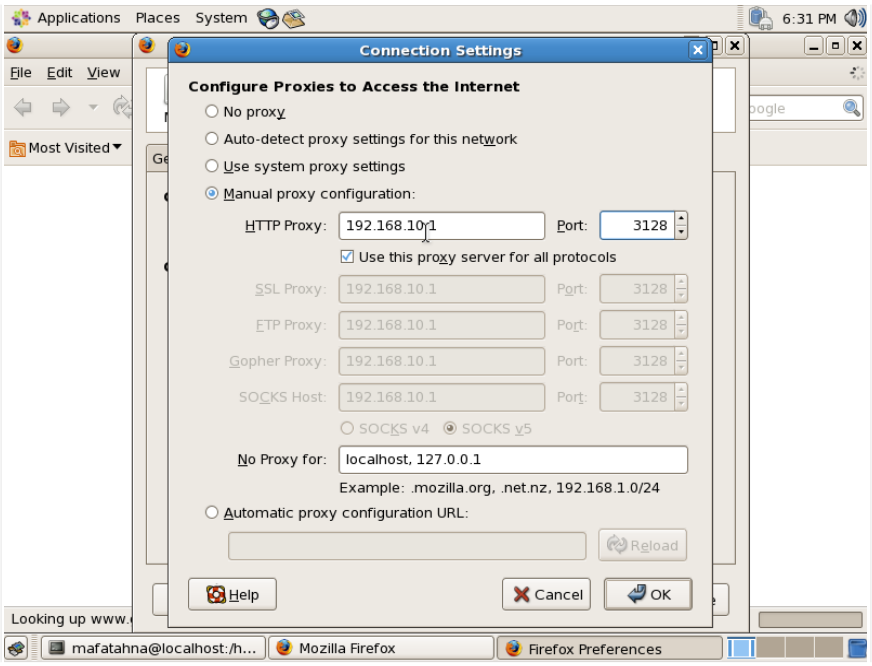
Selanjutnya aktifkan mode forwarding dengan mengubah default 0 menjadi 1 seperti dibawah ini

```
[root@proxy ~]# vim /etc/sysctl.conf
net.ipv4.ip_forward = 1
```

Simpan dan keluar dari editor tersebut, jalankan perintah dibawah ini

```
[root@proxy ~]# sysctl -p
net.ipv4.ip_forward = 1
net.ipv4.conf.default.rp_filter = 1
net.ipv4.conf.default.accept_source_route = 0
[root@proxy ~]#
```

Setelah mode forwarding sudah anda aktifkan, maka coba lakukan akses internet dari klien yaitu menambahkan proxy seperti dibawah ini



Jangan lupa untuk mengarahkan gateway ke IP Address router yaitu 192.168.10.1 sedangkan default port menggunakan 3128 sebab port squid tidak dirubah. Jika dari klien bisa akses internat maka proxy server anda sudah berhasil.

9.2. Authentikasi Password

Secara umum, klien yang terhubung dengan proxy server pasti bisa melakukan koneksi internet, dengan catatan mengetahui network, gateway dan DNS yang digunakan. Namun jika internet tersebut digunakan hanya untuk orang tertentu maka sistem tersebut kurang aman, sebab setiap orang bisa terkoneksi dengan internet. Authentikasi password digunakan solusi dari masalah tersebut.

Sistem ini biasa digunakan lingkup Universitas, sebab batasan dalam hak akses yang digunakan tidak lagi bersifat IP Address yang digunakan klien, tetapi menggunakan user dan password sehingga aktifitas internet lebih aman dan hanya orang-orang yang memiliki user dan password saja yang bisa menggunakan fasilitas internet.

Htpasswd merupakan sistem authentikasi dari apache, namun bisa di integrasikan dengan squid. Dalam penggunaanya juga relatif mudah sebab squid sudah support dengan htpasswd. Sebelum menambahkan beberapa parameter yang digunakan di file squid.conf, buatlah user yang digunakan untuk akses internet menggunakan htpasswd dengan perintah dibawah ini :

```
[root@proxy ~]# touch /etc/squid/password
[root@proxy ~]# htpasswd /etc/squid/password user1
New password:
Re-type new password:
Adding password for user user1
[root@proxy ~]#
```

Setelah user ditambahkan menggunakan htpassword, langkah selanjutnya menambahkan beberapa parameter yang terdapat di file squid.conf, edit file tersebut seperti berikut ini :

```
[root@proxy ~]# vim /etc/squid/squid.conf
```

Hilangkan tanda komentar [#] pada parameter dibawah ini :

```
auth_param basic program /usr/lib/squid/ncsa_auth /etc/squid/passwd
auth_param basic children 5
auth_param basic realm Squid proxy-caching web server
auth_param basic credentialsttl 2 hours
auth_param basic casesensitive off
```

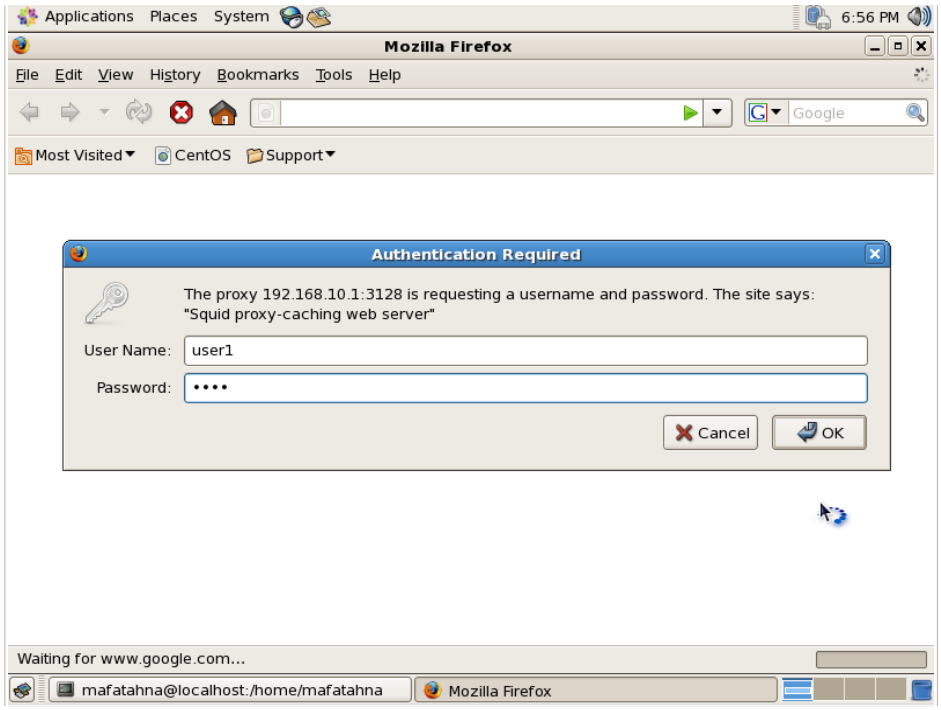
Tambahkan ncsa network dibawah acl network

```
acl my_network src 192.168.10.0/24
acl ncsa_network proxy_auth REQUIRED
```

Tambahkan juga hak akses dibawah acl network

```
http_access allow ncsa_network
http_access allow my_network
```

Simpan konfigurasi tersebut, keluar dari editor dan terakhir restart squid. Lakukan uji coba menggunakan web browser, jika dalam akses alamat situs meminta password dan user maka integrasikan htpassword dengan squid sudah berhasil.



Permintaan authentikasi tersebut digunakan sebagai kunci koneksi ke internet, sehingga jika terdapat user memasukkan user name dan password salah, maka secara otomatis akan ditolak oleh server proxy.

9.3. Filtering Content

Internet merupakan pintu untuk mengetahui semua informasi di dunia, banyak sekali kemudahan yang dihasilkan dari teknologi internet, namun informasi yang terdapat di internet tidak semuanya berdampak positif bagi kebanyakan orang, sehingga perlu adanya pemilihan content apa saja yang perlu dan tidak untuk diakses.

Penerapan fitur ini biasanya digunakan di beberapa Universitas yaitu dengan harapan fasilitas internet yang diberikan kampus hanya ditujukan terhadap situs-situs yang berhubungan dengan kampus, sehingga mahasiswa bisa lebih memaksimalkan dalam aktifitas mencari informasi dan mewujudkan internet sehat di Universitas tersebut.

Parameter yang digunakan dalam acl url_regex, sehingga jika anda memiliki list alamat situs yang di blok bisa dimasukkan terlebih dahuli pada sebuah file sehingga script yang ditambahkan di squid.conf lebih singkay. Dalam penerapannya anda bisa melihat contoh berikut ini :

Membuat file sebagai lokasi penulisan website yang di block

```
[root@proxy ~]# mkdir /etc/squid/block/
[root@proxy ~]# touch /etc/squid/block/acl_jejaringsosial
[root@proxy ~]# touch /etc/squid/block/acl_terlarang
```

Terdapat 2 file yang digunakan sebagai block content yaitu acl_jejaringsosial dan acl_terlarang, fungsi

dari file tersebut akan digunakan sebagai pengelompokan alamat website seperti jejaring sosial (facebook, twitter dll) sedangkan acl_terlarang digunakan sebagai pengelompokan situs-situs yang tidak diperbolehkan, misalnya situs torent dan situs porno.

Tambahkan beberapa alamat situs di kedua file tersebut dengan editor vim seperti dibawah ini :

```
[root@proxy ~]# vim /etc/squid/block/acl_jejaringsosial
.facebook.com
.twitter.com

[root@proxy ~]# touch /etc/squid/block/acl_terlarang
.youtube.com
```

Anda juga bisa menambahkan alamat situs yang lain sesuai kebutuhan, setelah file sudah tersedia maka anda tinggal pemasukkan parameter dibawah ini ke dalam file squid.conf

```
acl blokir1 url_regex -i "/etc/squid/block/acl_jejaringsosial"
acl blokir2 url_regex -i "/etc/squid/block/acl_terlarang"

http_access deny blokir1
http_access deny blokir2
```

Nama blokir1 hanya sebuah pendefinisian sehingga bisa anda ganti sesuai kebutuhan,

9.4. Limit Berdasarkan Waktu

Batasan akses internet akan lebih flexibel jika diterapkan terhadap beberapa waktu yang memang diharapkan sebagai user tidak jenuh yang hanya bisa mengakses beberapa situs yang sudah ditunjuk. Namun bisa juga digunakan sebagai (hiburan) ketika semua aktifitas sudah selesai. Misalnya sebuah Universitas menerapkan filtering content dengan aturan sebagai berikut

Block seluruh situs jejaring sosial pada jam praktikum yaitu
Jam 08:00 s.d 12:00 dan 13:00 s.d 16:00 hari Senin s.d Jum'at
Jam 08:00 s.d 12:00 hari Sabtu dan Minggu

Sedangkan situs terlarang di block permanen (setiap hari). Maka anda bisa menerapkan aturan tersebut dengan rule berikut ini :

```
acl waktu_pagi time MTWHF 08:00-12:00
acl waktu_siang time MTWHF 13:00-16:00
acl hari_libur time AS 08:00-14:00

acl blokir_situs url_regex -i "/etc/squid/block/acl_jejaringsosial"
acl blokir_terlarang url_regex -i "/etc/squid/block/acl_terlarang"

http_access deny blokir_situs waktu_pagi
http_access deny blokir_situs sabtu_siang
http_access deny blokir_situs hari_libur
http_access deny blokir_terlarang
```

Keterangan :
S – Sunday, M – Monday, T – Tuesday, W – Wednesday, H – Thursday, F – Friday, A – Saturday

9.5. Partisi Cache di Squid

Sebelumnya sudah dijelaskan cara membuat partisi cache di bab installasi pada buku ini. Cache digunakan sebagai tempat penyimpanan cache sementara, sehingga kecepatan dalam penyimpanan cache juga perlu diperhatikan sehingga perlu adanya partisi tersendiri sebagai media penyimpanan cache. Berikut ini langkah-langkah yang digunakan untuk menambahkan cache di squid.

Cek terlebih dahulu partisi di root (/) apakah sudah terdapat partisi cache atau belum, dengan perintah

```
[root@proxy ~]# ls /
bin      cache02  etc   lost+found  mnt  proc  selinux  tmp
boot     cache03  home  media       net  root  srv      usr
cache01  dev      lib   misc        opt  sbin  sys      var
[root@proxy ~]#
```

Selanjutnya ganti hak kepemilikan cache tersebut menjadi squid (sebelumnya root), dengan perintah chown seperti berikut ini :

```
[root@proxy ~]# chown squid.squid /cache01
[root@proxy ~]# chown squid.squid /cache02
[root@proxy ~]# chown squid.squid /cache03
```

Secara default cache sudah diarahkan ke direktoti /var/spool/squid edit pengaturan cache berikut ini :

```
#Default:
# cache_dir ufs /var/spool/squid 100 16 256
```

Menjadi

```
cache_dir ufs /cache01 3000 16 256
cache_dir ufs /cache02 3000 16 256
cache_dir ufs /cache03 3000 16 256
```

Simpan dan tutup file squid.conf, selanjutnya restart squid

9.6. Transparent Proxy

Layanan free akses internet yang disediakan di beberapa cafe, hotel dan restaurant biasanya tidak menggunakan password. Namun, jangan kira free hotspot tersebut tidak memiliki proxy yang digunakan untuk memonitoring aktifitas anda di internet, biasanya koneksi internet yang digunakan menggunakan salah satu fungsi dari squid yaitu proxy transparent.

Proxy transparent memungkinkan penggunaan bebas melakukan koneksi intenet tanpa memasukkan alamat proxy dan port yang digunakan. Namun klien akan dipaksa untuk masuk kedalam sistem squid terlebih dahulu sebelum terkoneksi dengan internet. Adapun langkah-langkah untuk membuat proxy transparent adalah sebagai berikut.

Aktifkan forwarding dengan memberikan angka 1 (aktif)

```
[root@proxy ~]# vim /etc/sysctl.conf
net.ipv4.ip_forward = 1
```

Selanjutnya aktifkan fitur tersebut dengan perintah berikut ini :

```
[root@proxy ~]# sysctl -p
net.ipv4.ip_forward = 1
net.ipv4.conf.default.rp_filter = 1
net.ipv4.conf.default.accept_source_route = 0
[root@proxy ~]#
```

Tambahkan default port yang terdapat di /etc/squid/squid.conf menjadi

```
http_port 3128 transparent
```

Simpan konfigurasi squid.conf, kemudian jalankan iptables untuk mengalihkan default port http (80) menuju port yang digunakan squid yaitu 3128. perintahnya adalah sebagai berikut ini :

```
[root@proxy ~]# iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
[root@proxy ~]# iptables -A PREROUTING -t nat -p tcp --dport 80 -j REDIRECT
--to-port 3128
```

Agar perintahnya tersebut dijalankan secara otomatis ketika komputer restart maka save rule tersebut ke file /etc/rc.local

```
[root@proxy ~]# vim /etc/rc.local

#!/bin/sh
#
# This script will be executed *after* all the other init scripts.
# You can put your own initialization stuff in here if you don't
# want to do the full Sys V style init stuff.

iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
iptables -A PREROUTING -t nat -p tcp --dport 80 -j REDIRECT

touch /var/lock/subsys/local
```

Simpan konfigurasi tersebut dan restart PC Router anda, lakukan uji coba dengan menghapus konfigurasi proxy di web browser klien.

9.7. Membatasi Bandwidth Dengan Delay Pools

Fitur-fitur yang dimiliki squid selain memiliki beberapa parameter yang digunakan sebagai batasan hak akses dan filter content, namun juga memili fitur yang digunakan sebagainya limit bandwidth yaitu delay pools. Delay pools sendiri memiliki beberapa struktur tambahan meliputi :

Delay_pools

Parameter ini digunakan sebagai dasar dalam manajemen bandwidth yaitu menentukan berapa jumlah pools yang akan digunakan, parameter ini nantinya akan berhubungan dengan parameter yang lain seperti delay_class, delay_parameters dan delay_access, kode yang digunakan yaitu :

```
delay_pools 3
```

Artinya dalam parameter delay pools menerapkan 3 pengelompokan manajemen bandwidth

Delay_class
Merupakan parameter yang digunakan untuk menentukan jumlah class dalam delay pools, squid pada dasarnya hanya mendukung 3 class saja yaitu

- Class 1 : berfungsi untuk membatasi bandwidth dalam jaringan dengan single bucket, opsi ini nanti juga bisa digunakan sebagai parent dari class sesudahnya yaitu class 2 dan class 3
- Class 2 : batasan jika menggunakan opsi ini akan dibatasi oleh single bucket (class 1) tetapi class 2 juga bisa memberikan batasan tersendiri dibawah parent (class 1) yaitu disetiap host.
- Class 3 : merupakan opsi class yang paling spesifik sebab class ini dibatas single bucket (class 1) dan batasan per host (class 2). Namun biasanya class 3 digunakan untuk membatasi file multimedia, document dan beberapa extension lain, misalnya mp3, odt, avi dan lain sebagainya.

Kode yang digunakan yaitu :

```
delay_class 1 3
```

Delay_parameters
Parameter yang digunakan untuk menentukan nilai yang digunakan sebagai limit bandwidth, misalnya :

```
delay_parameters 1 64000/64000 10000/320000 1000/1000
```

Dari contoh parameter tersebut dijelaskan bawah bandwidth total yang diberikan adalah 64000 bps, jika anda ingin mengubahnya kesatuan Kbps (Kilo Bit) silahkan dibagi 8, untuk lebih jelasnya perhatikan contoh berikut ini :

```
64000 bps (Bit) = 512 Kbps (Kilo Bit) = 64KBps (Kilo Byte)
```

Sehingga kecepatan real yang akan didapatkan adalah 64 KBps, dari penjelasan diatas merupakan hasil dari besar jumlah bandwidth yang diberikan dalam class 1 (single bucket). Delay class 2 terdapat 10000 dan 32000, artinya secara normal bandwidth yang didapatkan setiap host dalam jaringan adalah 80 Kbps dan 256 Kbps adalah nilai bandwidth maksimum dalam bucket. Delay class 3 lebih spefisik dengan batasan segment di jaringan seperti extension file dan multimedia.

Delay_access
Parameter yang terakhir di delay pools ini digunakan sebagai menentukan acl mana saja yang di ijinkan dalam mengikuti prosedur yang sudah ditetapkan dalam struktur delay pools. Misalnya anda memiliki acl yang di alokasikan untuk admin dan office, yang anda inginkan admin tidak melalui delay pools, namun office masuk dalam prosedur delay pools, maka parameter yang digunakan adalah :

```
delay_access 1 allow office
delay_access 2 deny admin
```

9.8. File Squid.conf

Berikut ini contoh parameter yang digunakan di squid sekaligus catatan singkat sebagai penjelasan, anda juga bisa copas ke server proxy anda tetapi dengan catatan file-file yang terdapat di konfigurasi tersebut juga harus ada misalnya acl_jejaringsosial, web, file, multimedia dan lain sebagainya.

```
# Mengaktifkan fitur authentikasi password
auth_param basic program /usr/lib/squid/ncsa_auth /etc/squid/password
auth_param basic children 5
auth_param basic realm Squid proxy-caching web server
auth_param basic credentialsttl 2 hours
auth_param basic casesensitive off

acl ncsa_network proxy_auth REQUIRED
acl waktu time MTWHF 08:00-16:00
acl sabtu time AS 08:00-14:00

# Redirect ke situs google.com jika mengakses situs jejaringsosial
# dalam jam kerja
acl blokir url_regex -i "/etc/squid/block/acl_jejaringsosial"
deny_info http://www.google.com blokir

# rule block situs website
acl blokir1 url_regex -i "/etc/squid/block/acl_terlarang"
acl blokir2 url_regex -i "/etc/squid/block/web"

# limitasi bandwidth berdasarkan extension
acl limit_download url_regex -i "/etc/squid/download/file"
acl limit_download url_regex -i "/etc/squid/download/multimedia"
acl limit_download url_regex -i "/etc/squid/download/software"

# acl user dalam groups
acl unlimited proxy_auth  "/etc/squid/groups/unlimited"
acl standart proxy_auth "/etc/squid/groups/standart"
acl limit proxy_auth "/etc/squid/groups/limit"
acl nointernet proxy_auth "/etc/squid/groups/nointernet"

acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl to_localhost dst 127.0.0.0/8
acl SSL_ports port 443
acl Safe_ports port 80          # http
acl Safe_ports port 21          # ftp
acl Safe_ports port 443         # https
acl Safe_ports port 70          # gopher
acl Safe_ports port 210         # wais
acl Safe_ports port 1025-65535  # unregistered ports
acl Safe_ports port 280         # http-mgmt
acl Safe_ports port 488         # gss-http
acl Safe_ports port 591         # filemaker
acl Safe_ports port 777         # multiling http
acl CONNECT method CONNECT
```

```
# block situs berdasarkan waktu yang sudah ditentukan
http_access deny blokir waktu
http_access deny blokir sabtu

# block situs pada rule blokir1
http_access deny blokir1

# user kelompok groups nointernet hanya bisa mengakses situs yang terdaftar
# di file blokir2 = /etc/squid/block/web
http_access allow blokir2
http_access deny nointernet

http_access allow unlimited
http_access allow standart
http_access allow limit

# Mengaktifkan fitur authentikasi
http_access allow ncsa_network

http_access deny manager localhost
http_access deny manager
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access deny localhost
http_access deny all

icp_access allow all
http_port 3128
hierarchy_stoplist cgi-bin ?

cache_mem 8 MB
maximum_object_size_in_memory 8 KB
memory_replacement_policy lru
cache_replacement_policy lru

# partisi cache
cache_dir ufs /cache01 3000 16 256
cache_dir ufs /cache02 3000 16 256
cache_dir ufs /cache03 3000 16 256

minimum_object_size 0 KB
maximum_object_size 4096 KB
cache_swap_low 90
cache_swap_high 95
access_log /var/log/squid/access.log squid
cache_log /var/log/squid/cache.log
cache_store_log /var/log/squid/store.log
logfile_rotate 0
mime_table /etc/squid/mime.conf
```

```
acl QUERY urlpath_regex cgi-bin \?
cache deny QUERY
refresh_pattern ^ftp:           1440    20%     10080
refresh_pattern ^gopher:        1440    0%      1440
refresh_pattern .               0       20%     4320
quick_abort_min 16 KB
quick_abort_max 16 KB
quick_abort_pct 95
positive_dns_ttl 1 hours
negative_dns_ttl 1 minute
request_header_max_size 20 KB
reply_header_max_size 20 KB
request_body_max_size 0 KB
acl apache rep_header Server ^Apache
broken_vary_encoding allow apache
cache_mgr root
forwarded_for on
coredump_dir /var/spool/squid

header_access Referer deny all
header_access X-Forwarded-For deny all
header_access Via deny all
header_access Cache-Control deny all

delay_pools 4

# Membatas download di file extensi yang sudah diregistrasikan
# dengan bandwidth penuh 256 kbps, perhost 80kbps sedangkan
# per extension 8kbps
delay_class 1 3
delay_parameters 1 32000/32000 10000/10000 1000/1000
delay_access 1 allow limit limit_download
delay_access 1 deny all

# Bandwidth yang disediakan 256kbps sedangkan untuk perhost 80kbps
delay_class 2 2
delay_parameters 2 32000/32000 10000/10000
delay_access 2 allow limit
delay_access 2 deny all

# Bandwidth yang disediakan 512kbps sedangkan untuk perhost 256kbps
delay_class 3 2
delay_parameters 3 64000/64000 32000/32000
delay_access 3 allow standart
delay_access 3 deny all

# Bandwidth yang disediakan unlimited
delay_class 4 1
delay_parameters 4 -1/-1
delay_access 4 allow unlimited
delay_access 4 deny all
```