

Step By Step Konfigurasi Squid Proxy Server dengan Berbagai Studi Kasus

Bagian 1 dari 2 Artikel

Proxy Server adalah server yang berguna sebagai perantara antara *client* dengan server gateway sebelum berhubungan ke Internet. Dengan adanya proxy server ini, maka url / situs yang sering di-*browsing* akan semakin terasa semakin cepat terakses oleh user, karena telah disimpan di dalam *cache proxy*. Selain itu, proxy server juga memiliki fungsi lainnya, di antaranya autentifikasi user, memblok situs, memblok *banner*, dan lain-lain.

Bagi para administrator warnet atau kantor, pasti pernah berpikir bagaimana caranya agar *loading* situs yang dibuka oleh user terasa lebih cepat, dapat memblok situs-situs porno yang sering membawa *spyware*, membatasi ukuran *download* file user, autentifikasi user mana saja yang diperbolehkan *browsing*, me-*redirect* suatu situs porno ke situs yang lain, dan sebagainya.

Jika itu permasalahanannya, maka jawabannya adalah si administrator dapat membuat sebuah mesin proxy server untuk menjembatani hubungan dari Internet ke user. Mesin proxy ini akan bertindak sebagai pemfilter paket yang datang dari Internet, baik itu melalui port http atau ftp, sebelum sampai ke user. Salah satu software proxy terbaik yang ada di GNU/Linux adalah Squid. Squid adalah software proxy server open source dengan banyak fitur.

Pada artikel kali ini, penulis akan menjelaskan cara konfigurasi Squid untuk:

1. Memberi hak akses Internet agar hanya dapat digunakan oleh komputer dengan nomor IP tertentu.
2. Memblok situs terlarang secara manual.
3. Memblok situs terlarang dengan menggunakan program redirector Squid-Guard.

4. Memblok banner menggunakan redirector adzap.
5. Membatasi ukuran file (kuota) yang bisa di-download oleh user pada interval waktu tertentu.
6. Autentifikasi user.
7. Transparant Proxy.

Adapun distro yang dipakai penulis dalam menyusun penulisan ini adalah Fedora Core 3, dan seharusnya dapat di terapkan juga pada pengguna distro lainnya. Untuk mempersingkat waktu, silakan baca langkah-langkahnya di bawah ini:

Instalasi Squid Proxy Server

- Instalasi software Squid Proxy Server dapat dilakukan dari *source* ataupun yang sudah berbentuk binary. Untuk petunjuk instalasi Squid dari *source* dapat Anda lihat pada file INSTALL yang terdapat pada tarball squid.
- Diasumsikan Anda sudah menginstallasikan Fedora Core 3 di komputer Anda. Dan bagi pengguna distro lain, Anda tinggal menyesuaikan langkah-langkahnya saja.
- Selanjutnya adalah lihat di Sistem Linux anda, apakah Squid sudah terinstalasi di Sistem Linux Anda.

- Check dengan mengetikkan perintah di bawah ini dari konsol :

```
# rpm -qa | grep squid
```

- Jika sudah ada, lanjut ke bagian konfigurasi, jika belum ada, ikuti langkah instalasi squid di bawah ini.
- Masuk ke Menu Utama, System Settings, Add/Remove Application. Masukkan password root Anda. Setelah tampil menu *Add or Remove Packages*, lihat dibagian *Servers*, lalu klik bagian *Web Server*, klik *Details*, lalu check di bagian software squid. Klik tombol *Update*. Masukkan CD sesuai dengan permintaan *installer*.

Konfigurasi squid proxy server

Selanjutnya kita akan mulai mengonfigurasi squid, pertama, buat direktori cache.

(Catatan : tanda # berarti perintah dijalankan oleh root user).

```
# cd /
# mkdir /cache
# chown squid.squid /cache -Rf
```

Setelah membuat direktori /cache, selanjutnya kita mulai mengonfigurasi squid.

```
# cd /etc/squid
```

```
# mv squid.conf squid.conf.bak
# touch squid.conf
# chmod 640 squid.conf
```

Berikutnya, penulis akan menjelaskan konfigurasi squid sesuai dengan kriteria yang telah penulis jelaskan.

1. Konfigurasi Squid untuk membatasi hak akses Internet agar hanya dapat digunakan oleh komputer dengan nomor IP tertentu.

Studi Kasus :

Misalkan di suatu PT XYZ terdapat tiga buah divisi. Sebut saja divisi perusahaan tersebut dengan DivisiA, DivisiB, dan DivisiC.

- DivisiA memiliki IP range antara 192.168.0.20 – 192.168.0.60
- DivisiB memiliki IP range antara 192.168.0.61 – 192.168.0.100
- DivisiC memiliki IP range antara 192.168.0.101 – 192.168.0.140

Persyaratannya :

1. PT XYZ ingin agar DivisiA dan DivisiB memiliki hak akses ke Internet.
2. PT XYZ ingin agar DivisiC tidak memiliki hak akses ke Internet.
3. Komputer salah seorang staf yang ada di divisi C, yang memiliki IP 192.168.0.130 dibolehkan memiliki hak akses ke Internet.

Untuk memenuhi persyaratan tersebut, cobalah untuk mengedit file squid.conf, seperti di bawah ini :

```
# vi squid.conf

# port (bagian ini berisikan port yang akan digunakan oleh squid)
http_port 3128
icp_port 3130
tcp_outgoing_address 0.0.0.0
udp_incoming_address 0.0.0.0
udp_outgoing_address 0.0.0.0

# cache_peer (bagian ini berisikan hubungan proxy server yang ada dilokal ke server # proxy lainnya. Hubungan ini terdiri atas dua jenis yaitu parent dan sibling).
# Sesuaikan atau tanyakan alamat
```

cache_peer ini sesuai dengan ISP yg anda gunakan.

```
cache_peer proxies.telkom.net.id
parent 8080 3130 default
```

```
cache_peer proxy-sby.telkom.net.id
id sibling 8080 3130 round-robin
```

```
# memory (bagian ini berisikan besarnya memori yang akan digunakan oleh squid
```

```
# untuk menyimpan in transit object dan hot object).
```

```
# Besar angka yang aman dipakai adalah ¼ dari jumlah memori yang ada.
```

```
cache_mem 32 MB
```

```
# direktori (bagian ini berisikan tentang direktori yang akan digunakan sebagai tempat penyimpanan cache/ objek website squid).
```

```
# Maksud perintah dibawah ini adalah : pertama jenis file system yang dipakai adalah ufs, lalu /cache adalah nama direktorinya. Ukuran cache sebesar 1000 MB, lalu 16 dan 256 adalah jumlah direktori yang terdapat di dalam /cache pada level 1 dan 2.
```

```
cache_dir ufs /cache 1000 16 256
```

```
# log (bagian ini berisikan tentang lokasi file log yang akan digunakan squid).
```

```
cache_access_log /var/log/squid/access.log
```

```
cache_log /var/log/squid/cache.log
```

```
cache_store_log /var/log/squid/store.log
```

```
client_netmask 255.255.255.0
```

```
unlinkd_program /usr/lib/squid/unlinkd
```

```
#refresh pattern
```

```
refresh_pattern ^ftp: 1440 20% 10080
```

```
refresh_pattern ^gopher: 1440 0% 1440
```

```
refresh_pattern . 0 20% 4320
```

```
# acl definisi (bagian ini berisikan batasan-batasan yang akan dilakukan oleh server squid).
```

```
# Dan bagian ini adalah inti dari penerapan kebijakan yang ada di proxy server
```

```
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
```

```
acl SSL_ports port 443 563
```

```
acl Safe_ports port 80 21 443 563 70 210 1025-65535
```

```
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
```

```
acl divisia src 192.168.0.20-192.168.0.60/255.255.255.255
```

```
acl divisib src 192.168.0.61-192.168.0.100/255.255.255.255
```

```
acl divisiC src 192.168.0.101-192.168.0.140/255.255.255.255
```

```
acl udinc src 192.168.0.130/255.255.255.255
```

```
# rule (bagian ini berisikan keterangan untuk membiarkan atau menolak bagian acl # yang telah dibuat).
```

```
http_access allow manager
```

```
http_access allow localhost
```

```
http_access allow udinc
```

```
http_access allow divisia
```

```
http_access allow divisib
```

```
http_access deny divisiC
```

```
http_access deny !Safe_ports
```

```
http_access deny CONNECT !SSL_ports
```

```
http_access deny all
```

```
#http_reply_access
```

```
http_reply_access allow all
```

```
# icp access
```

```
icp_access allow all
```

```
# display message
cache_mgr supriyanto@infolinux.
co.id
cache_effective_user squid
cache_effective_group squid
visible_hostname infolinux.co.id
```

Setelah itu *Save*, dan *restart* service squid untuk melihat perubahan yang telah dilakukan.

```
# service squid restart
```

Sekarang coba tes, apakah *setting*-an yang telah anda simpan telah berhasil. Caranya, masukkan dahulu setting HTTP proxy dan portnya di *web browser* user Divisi C. Di Mozilla Firefox Anda bisa men-setting-nya dari menu *Edit, Preferences*. Di Tab General, klik *Connection Settings*. Isikan HTTP Proxy dan Port-nya, sesuai dengan IP server proxy Anda dan port proxy yang digunakan.

Jika komputer dengan IP divisi C keculi komputer yang memiliki IP 192.168.0.30 tidak bisa membuka halaman situs, berarti langkah-langkah yang anda lakukan sudah benar. Coba juga di salah satu user yang ada di DivisiA atau DivisiB, jika user ini bisa membuka halaman situs berarti tidak ada masalah pada konfigurasi squid yang telah dibuat, atau dengan kata lain Anda telah berhasil men-setting squid untuk kasus pertama.

2. Memblok situs terlarang secara manual.

Studi kasus:

PT XYZ memiliki suatu problem di mana banyak karyawannya yang “dewasa” suka

membuka situs-situs porno pada waktu jam kerja. Hal ini tentunya membuat risih beberapa pegawai lainnya dan dapat menurunkan image perusahaan. Maka dari itu, PT XYZ ingin membuat suatu aturan untuk pemfilterannya yang datang dari Internet sebelum sampai ke user.

Persyaratannya:

1. PT XYZ ingin agar semua komputer Divisi A dan Divisi B yang terhubung ke Internet tidak dapat mengakses situs-situs terlarang yang telah didefinisikan oleh administrator.
2. PT XYZ ingin agar beberapa komputer yang ada di Divisi A yang memiliki *range* IP dari 192.168.0.20 – 192.168.0.30 dapat mengakses ke situs apa saja yang ada di Internet (tidak termasuk ke dalam persyaratan 1).
3. PT XYZ menginginkan juga IP situs porno tersebut juga diblok. Karena biasanya jika si user sudah ahli, maka hanya dengan mengetikkan alamat IP-nya langsung di kolom alamat Url yang ada di web browser, situs porno tersebut tetap dapat diakses.
4. PT XYZ menginginkan juga agar kalimat-kalimat yang berbaur porno, yang dimasukkan oleh user melalui *search engine* atau alamat situs, dapat langsung terblokir oleh proxy server.

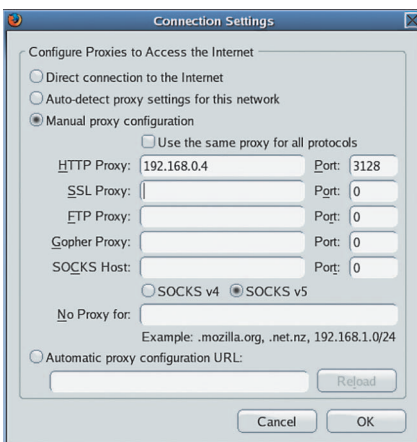
Untuk memenuhi persyaratan tersebut, cobalah untuk mengedit file *squid.conf*, seperti di bawah ini :

```
# vi squid.conf
.....
.....
.....
# acl definisi (bagian ini
berisikan batasan-batasan yang
akan dilakukan oleh server
# squid).
# Dan bagian ini adalah inti
dari penerapan kebijakan yang
ada di proxy server
acl domainterlarang dstdomain “/
etc/squid/domain-terlarang.txt”
acl kataterlarang url_regex -i
“/etc/squid/kata-terlarang.txt”
acl ipterlarang dst “/etc/squid/
ip-terlarang.txt”
```

```
acl myNet src 192.168.0.0/255.
255.255.255
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 SSL_ports port 443 563
acl Safe_ports port 80 21 443
563 70 210 1025-65535
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
acl divisia src 192.168.0.20-
192.168.0.60/255.255.255.255
acl divisib src 192.168.0.61-
192.168.0.100/255.255.255.255
acl divisic src 192.168.0.101-
192.168.0.140/255.255.255.255
acl bebasbuka src 192.168.0.20-
192.168.0.30/255.255.255.255
acl udinc src 192.168.0.130/255.
255.255.255
```

```
# rule (bagian ini berisikan
keterangan untuk membiarkan atau
menolak bagian acl
# yang telah dibuat).
http_access deny domainterlarang
!bebasbuka
http_access deny kataterlarang
!bebasbuka
http_access deny ipterlarang
!bebasbuka
http_access allow manager
http_access allow localhost
http_access allow udinc
http_access allow divisia
http_access allow divisib
http_access deny divisic
http_access deny !Safe_ports
http_access deny CONNECT !SSL_
ports
http_access deny all
```

```
#http_reply_access
http_reply_access allow all
.....
.....
```



Sesuaikan dengan settingan IP proxy server anda.

Setelah itu Save, dan buat tiga buah file yang bernama domain-terlarang.txt, kata-terlarang.txt, dan ip-terlarang.txt di direktori /etc/squid.

```
# cd /etc/squid
# touch domain-terlarang.txt
# touch kata-terlarang.txt
# touch ip-terlarang.txt
# vi domain-terlarang.txt
17tahun.com
www.playboy.com
www.nude.com
www.sex.com
www.porn.com
www.hardcore.com
```

➔ dan seterusnya, yang menurut Anda adalah domain situs porno.

```
# vi kata-terlarang.txt
```

```
sex
lesbian
lolita
homo
xxx
hot
17tahun
porn
```

➔ dan seterusnya, yang menurut Anda adalah kata-kata yang menunjuk ke situs porno.

```
# vi ip-terlarang.txt
```

```
70.84.171.179
216.163.137.3
64.74.96.243
209.81.7.23
213.193.215.179
216.130.180.165
```

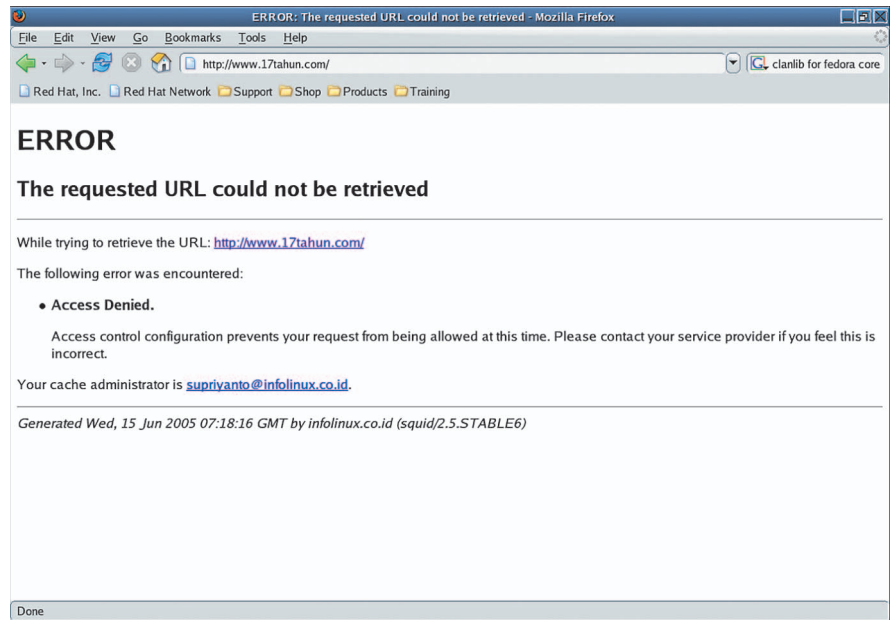
➔ dan seterusnya, yang menurut Anda adalah ip-ip yang menunjuk ke situs porno.

Restart service squid untuk melihat perubahan yang telah dilakukan.

```
# service squid restart
```

Test setting-an squid yang telah kita buat, misal dari browser mozilla firefox yang telah Anda setting dahulu http proxy dan port-nya.

1. Ketikkan di url, www.google.com, lalu test dengan mengisikan kalimat sex. Jika hasilnya adalah tulisan ERROR, berarti squid telah berhasil memblokir situs ber-



Tampilan Access Denied Dari Squid.

dasarkan kata yang telah anda definisikan di file kata-terlarang.txt

2. Ketikkan di alamat url alamat IP suatu situs, misal : 70.84.171.179. Jika hasilnya adalah tulisan ERROR, berarti squid telah berhasil memblokir situs berdasarkan ip yang telah Anda definisikan di file ip-terlarang.txt

3. Ketikkan di alamat url nama suatu situs, misal : www.17tahun.com. Jika hasilnya adalah tulisan ERROR, berarti squid telah berhasil memblokir situs berdasarkan nama situs yang telah Anda definisikan di file domain-terlarang.txt

4. Test sekali lagi dengan mengetikkan url situs yang tidak termasuk ke dalam salah satu situs yang diblok. Jika situs tersebut dapat diakses berarti settingan squid tersebut sudah memenuhi semua persyaratan yang diajukan.

5. Test di salah satu komputer yang ber-IP 192.168.0.20-192.168.0.30, jika komputer tersebut dapat membuka salah satu situs yang di-blok, berarti semua persyaratan sudah terpenuhi.

Untuk lebih pastinya, Anda dapat mengecek log squid Anda, untuk memastikan apakah situs yang dimaksud telah terblokir atau belum.

```
# tail -f /var/log/squid/store.log
1119498364.368 510
```

```
192.168.0.34 TCP_DENIED/403 1393
GET http://www.17tahun.com/ -
NONE/- text/html
1119498365.737 369
192.168.0.34 TCP_DENIED/403 1415
GET http://www.17tahun.com/
favicon.ico - NONE/- text/html
```

3. Memblok situs terlarang menggunakan program redirector SquidGuard

Pada studi kasus kedua, Anda telah mempelajari bagaimana cara memblokir suatu situs secara manual. Yaitu dengan menambahkan daftar nama situs, daftar IP situs, maupun kalimat secara manual. Mungkin kalau jumlah situs yang ingin kita blok masih berjumlah puluhan, hal tersebut tidak menjadi masalah buat administrator. Tapi perlu diingat bahwa jumlah situs jenis ini di Internet sangat banyak jumlahnya. Apalagi user biasanya masih saja ada yang dapat membuka situs porno, entah itu dari link yang dia dapat saat surfing maupun dari situs-situs *hacking* yang banyak bertebaran di Internet.

Pertanyaannya, apakah ada program yang menyediakan database situs terlarang yang dapat diintegrasikan ke Squid? Jawabannya ada. Anda dapat menggunakan salah satu program redirector Squid yang bernama SquidGuard.

SquidGuard berguna untuk mengindeks url-url porno, hacking, drugs, dan lain-lain.

Dengan SquidGuard ini, kita tidak perlu bersusah payah lagi mencari dan menuliskan domain-domain porno ke dalam suatu file, karena database squidguard sudah menyediakan puluhan ribu situs porno dan yang lainnya, yang didapat melalui *scripts robots* yang dibuat dengan bahasa PERL.

Untuk lebih jelasnya, penulis akan menjelaskan *step-by-step* pemakaian SquidGuard.

1. Diharapkan Anda telah sukses menjalankan studi kasus pertama dan kedua.
2. Pada studi kasus kali ini berbeda dengan kasus sebelumnya. Studi kasus kali ini dimisalkan semua komputer yang ada di semua divisi PT XYZ termasuk ke dalam jaringan yang terkena *content filtering* yang dilakukan oleh SquidGuard.
3. Download terlebih dahulu paket RPM SquidGuard untuk Fedora Core 3 pada url berikut:

<http://dag.wieers.com/packages/squid-guard/>

Atau Anda dapat mencarinya pada CD Majalah *InfoLinux* edisi ini.

4. Install paket tersebut dari konsol.

```
# rpm -ivh squidguard-1.2.0-2.1.fc3.rf.i386.rpm
```

5. Berikutnya ubah hak akses directory log squidGuard menjadi milik user Squid.

```
# chown squid.squid /var/log/squidguard -Rf
```

6. Berikutnya konfigurasi squidGuard. Diasumsikan situs-situs yang termasuk dalam database squidguard akan di-redirect ke situs <http://www.erasmuslim.com/>. Anda dapat merubah alamat url tersebut sesuai dengan keinginan anda.

```
# vi /etc/squid/squidguard.conf
```

```
# Konfigurasi ini didapat dari http://squidguard.mesd.k12.or.us/
```

```
# Author By : supriyanto@infoLinux.co.id
```

```
dbhome /var/lib/squidguard
logdir /var/log/squidguard
```

```
dest adult {
    log                adult
    domainlist         adult/
    domains
    urlist             adult/urls
}
```

```
dest drugs {
    log                drugs
    domainlist         drugs/
    domains
    urlist             drugs/urls
}
```

```
acl {
    default {
        pass !adult !drugs all
        redirect 302:http://www.erasmuslim.com
    }
}
```

Setelah kita konfigurasi file */etc/squidguard.conf*, berikutnya check apakah konfigurasi tersebut masih terdapat kesalahan atau tidak.

```
# /usr/bin/squidguard -v
SquidGuard: 1.2.0 Sleepycat
Software: Berkeley DB 4.2.52:
(March 2, 2004)
```

Kalau masih terdapat pesan kesalahan, betulkan konfigurasi *squidguard.conf* tersebut sampai benar.

1. Berikutnya edit file *squid.conf* pada bagian redirect program sehingga seperti di bawah ini :

```
# vi /etc/squid/squid.conf

..

# log (bagian ini berisikan tentang lokasi file log yang akan digunakan squid).
cache_access_log /var/log/squid/access.log
cache_log /var/log/squid/cache.log
cache_store_log /var/log/squid/store.log
client_netmask 255.255.255.0
unlinkd_program /usr/lib/squid/unlinkd

# redirect program (bagian ini berisikan program tambahan yang akan digunakan squid).
# untuk meningkatkan kinerja squid).
redirect_program /usr/bin/squidguard
redirect_children 5

#refresh pattern
refresh_pattern ^ftp: 1440 20% 10080
refresh_pattern ^gopher: 1440 0% 1440
refresh_pattern . 0 20% 4320
```

Amati file *access.log* squid untuk melihat status yang terjadi.

```
# acl definisi (bagian ini
berisikan batasan-batasan yang
akan dilakukan oleh server
# squid).
# Dan bagian ini adalah inti
dari penerapan kebijakan yang
ada di proxy server
acl myNet src 192.168.0.0/255
.255.255.0
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 SSL_ports port 443 563
acl Safe_ports port 80 21 443
563 70 210 1025-65535
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

# rule (bagian ini berisikan
keterangan untuk membiarkan
atau menolak bagian acl
# yang telah dibuat).
http_access allow manager
http_access allow localhost
http_access deny !Safe_ports
http_access deny CONNECT
!SSL_ports
http_access deny all

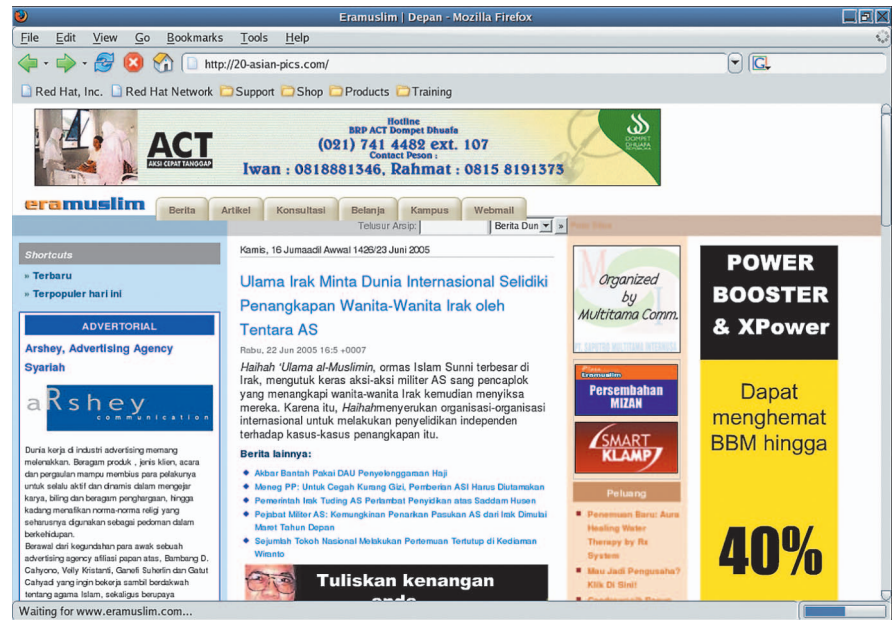
#http_reply_access
http_reply_access allow all

# icp access
icp_access allow all

# display message
cache_mgr
supriyanto@infolinux.co.id
cache_effective_user squid
cache_effective_group squid
visible_hostname infolinux.
co.id
```

2. Restart service squid Anda:

```
# service squid restart
```



Squid me-redirect situs porno ke Eramuslim.com.

3. Lihat di daftar proses, apakah kedua program redirector squid ini, sudah berjalan dengan baik.

```
# ps ax | grep squid

7542 ? Ss 0:00 squid -D
7544 ? S 0:01 (squid) -D
7546 ? Ss 0:00 (squidguard)
7547 ? Ss 0:00 (squidguard)
7548 ? Ss 0:00 (squidguard)
7549 ? Ss 0:00 (squidguard)
7550 ? Ss 0:00 (squidguard)
```

Dapat dilihat pada daftar proses di atas, bahwa program redirector squidguard sudah berjalan.

Cek juga daftar log squidguard, apakah benar-benar sudah berjalan dengan baik atau belum.

```
# tail -f /var/log/squidguard/
squidGuard.log

2005-06-23 10:54:47 [4072]
squidGuard 1.2.0 started
(1119498886.074)
2005-06-23 10:54:47 [4072]
squidGuard ready for requests
(1119498887.600)
```

4. Selanjutnya, lihatlah daftar situs-situs yang ada dalam database squidguard. Biasanya daftar situs tersebut di squidguard bernama *domains* dan letaknya

ada dalam kategori database situs squidguard. Sebagai contoh, saya akan melihat daftar situs porno yang termasuk sebagai kategori adult pada squidguard.

```
# cd /var/lib/squidguard
```

masuk ke directory kategori adult

```
# cd adult
```

```
# vi domains
```

Coba Anda lihat salah satu situs yang ada di file domains, lalu test dibuka dari browser salah satu user.

Sebagai contoh, ada situs <http://20-asian-pics.com> dalam file domains tersebut. Kita akan test apakah squidguard sudah berjalan dengan baik atau belum. Caranya:

Ketik <http://20-asian-pics.com> di browser anda. Lalu perhatikan hasil situs yang terbuka.

Jika yang terbuka adalah situs www.eramuslim.com, berarti squidguard sudah berjalan dengan baik di sistem anda. Atau dengan kata lain sudah berhasil untuk meredirect situs <http://20-asian-pics.com> menjadi situs www.eramuslim.com.

Sampai di sini dahulu pembahasan mengenai konfigurasi Squid. Bulan depan penulis akan melanjutkan dengan studi kasus berikutnya, yaitu studi kasus keempat sampai studi kasus ketujuh. Sampai jumpa. **Supriyanto** (supriyanto@infolinux.co.id)

Step By Step Konfigurasi Squid Proxy Server dengan Berbagai Studi Kasus

Bagian 2 dari 2 Artikel

Proxy server adalah server yang berguna sebagai perantara antara *client* dengan server gateway sebelum berhubungan ke Internet. Dengan adanya proxy server ini, maka url / situs yang sering di-*browsing* akan semakin terasa semakin cepat terakses oleh user, karena telah disimpan di dalam *cache proxy*. Selain itu, proxy server juga memiliki fungsi lainnya, di antaranya autentifikasi user, memblok situs, memblok *banner*, dan lain-lain.

Proxy server adalah server yang berguna sebagai perantara antara *client* dengan server gateway sebelum berhubungan ke Internet. Dengan adanya proxy server ini, maka url / situs yang sering di-*browse* akan semakin terasa semakin cepat terakses oleh user, karena telah disimpan di dalam squid cache. Selain itu, proxy server juga memiliki fungsi lainnya, di antaranya autentifikasi user, memblok situs, memblok *banner*, dan lain-lain.

Pada edisi sebelumnya, saya sudah menjelaskan tentang cara pengonfigurasi Squid dengan membahas studi kasus pertama sampai dengan ketiga. Sesuai dengan janji penulis sebelumnya, sekarang akan melanjutkannya dengan studi kasus keempat sampai dengan ketujuh. Dan studi kasus yang akan dibahas kali ini, yaitu:

4. Memblok banner menggunakan redirector adzap.
5. Membatasi ukuran file (kuota) yang bisa di-download oleh user pada interval waktu tertentu.
6. Autentifikasi user.
7. Transparant Proxy.

Untuk mempersingkat waktu, Anda dapat dapat langsung membaca tutorial di bawah ini:

4. Memblok banner situs menggunakan redirector adzap.

Pernahkah Anda membuka situs terkenal seperti *yahoo mail*, *detik.com*, ataupun situs terkenal yang lainnya? Kalau Anda pernah membuka situs tersebut, pasti akan melihat banyaknya *banner* yang menempel di situs tersebut. Dengan terbukanya banner, sebetulnya kita telah membuang *bandwidth* dengan sia-sia hanya untuk menampilkan banner itu.

Lalu, adakah program redirector squid yang dapat digunakan untuk memblok banner? Tentu ada, untuk melakukan hal tersebut Anda dapat menggunakan salah satu program redirector squid yang bernama adzap. Dengan adzap gambar banner yang ada akan diubah menjadi tulisan adzap.

Untuk pembahasan lebih lanjut bagaimana *setting* redirector adzap dan squidguard dapat berjalan bersamaan atau dengan kata lain bagaimana menggunakan multiple redirector, ikuti langkah-langkah di bawah ini:

1. Download program adzap dari internet.
<http://adzapper.sourceforge.net/adzap-20050605.tar.gz>
2. Pastikan perl, apache dan segala yang berkenaan dengan program ini sudah

terinstalasi dengan baik di sistem Anda.

```
# perl -v
```

3. Berikutnya, extract source adzap yang telah Anda download tersebut, ke directory /usr/local.

```
# tar -xzf adzap-20050605.tar.gz -C /usr/local
# cd /usr/local/adzap
```

Copy file-file berikut ke Document Root Apache anda, misal di Fedora Core 3 terletak di /var/www/html

```
# cd /var/www/html
# mkdir adzap
# cd adzap
# cp /usr/local/adzap/zaps/*.gif /var/www/html/adzap
# cp /usr/local/adzap/zaps/*.html /var/www/html/adzap
# cp /usr/local/adzap/zaps/*.js /var/www/html/adzap
```

4. Edit file wrapzap yang ada di /usr/local/adzap/scripts, pada bagian:

```
zapper=/usr/local/adzap/scripts/squid_redirect
ZAB_BASE=http://localhost/adzap
.....
```



```
.....
#exec "$zapper"
# exec /path/to/zapchain
"$zapper" /path/to/another/
eg/squirm
exec /usr/local/adzap/scripts/
zapchain "$zapper" /usr/bin/
squidguard
```

5. Edit squid.conf, tambahkan baris berikut:

```
.....
#-----
# redirect program (bagian ini
berisikan program tambahan
yang akan digunakan
# untuk meningkatkan kinerja
squid).
#Disini squid memanggil
program wrapzap yang akan
menjalankan dua buah #program
redirector yang dipanggil
oleh wrapzap yaitu redirector
squid_re dan #redirector
squidguard

redirect_program /usr/local/
adzap/scripts/wrapzap
redirect_children 5
#-----

#refresh pattern
refresh_pattern ^ftp: 1440
20% 10080
refresh_pattern ^gopher: 1440
```

```
0% 1440
refresh_pattern . 020% 4320
.....
```

6. Setelah selesai, *restart* service squid Anda

```
# service squid restart
```

7. Jalankan juga service apache Anda.

```
# service httpd start
```

8. Check apakah redirector adzap dan re-director squid guard sudah berjalan dengan baik.

```
# ps ax | grep squid_re
.....
9153 ? Ss 0:00 /usr/
bin/perl /usr/local/adzap/
scripts/zapchain /usr/local/
adzap/scripts/squid_redirect
/usr/bin/squidguard
9156 ? Ss 0:00
/usr/bin/perl /usr/local/
adzap/scripts/zapchain /usr/
local/adzap/scripts/squid_
redirect /usr/bin/squidguard
/usr/bin/perl -w /usr/local/
adzap/scripts/squid_redirect
9164 ? S 0:00
/usr/bin/squidguard
9168 ? S 0:01
/usr/bin/perl -w /usr/local/
adzap/scripts/squid_redirect
.....
```

9. Test ke browser, dengan mengetikkan situs yang terdapat banyak banner, misal: www.detik.com, jika Anda melihat banner yang terdapat pada situs detik.com telah berubah menjadi tulisan This AdZaped, berarti Anda telah berhasil mengonfigurasi squid untuk memblokir banner iklan.

10. Test juga dengan mengetikkan salah satu situs yang termasuk ke dalam daftar blacklist squidguard (ex:// <http://20-asian-pics.com>). Jika situs tersebut ter-redirect ke situs <http://www.erasmuslim.com>, artinya Anda telah dapat menjalankan multiple redirector squid secara bersamaan.

Bahkan jika ingin menambahkan program redirector squid yang lain, Anda hanya perlu menambahkan path programnya di file wrapzap.

11. Untuk melihat log file, url yang berhasil di blok banner-nya, Anda dapat mengetikkan perintah berikut :

```
# tail -f /var/log/httpd/
access_log
```

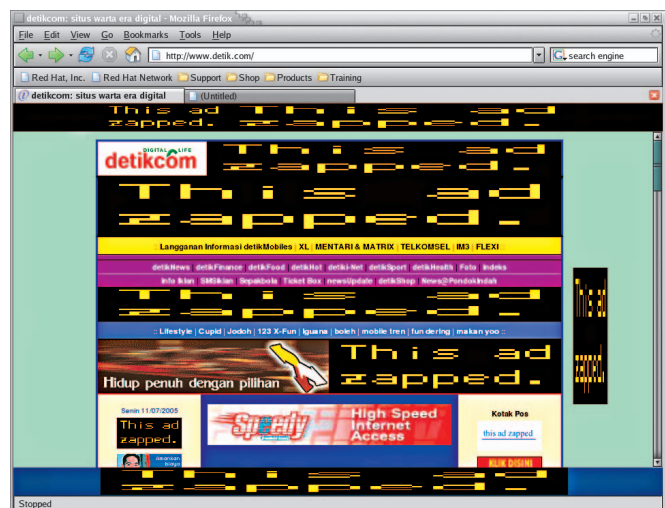
5. Membatasi ukuran file (kuota) yang bisa di-download oleh user pada interval waktu tertentu.

Setelah melihat beberapa studi kasus di atas, mungkin ada peningkatan kecepatan pada waktu akses suatu sites yang dibuka oleh user. Apalagi kalau situs tersebut sudah terdaftar kedalam cache squid.

Selain itu, kecepatan akses juga bergantung pada jalur bandwidth yang anda sewa



Banner situs yang belum diblok sebelum menggunakan adzap.



Banner situs yang telah diblok setelah menggunakan adzap.

dari ISP. Lalu ada juga faktor yang paling penting yang paling berpengaruh pada waktu akses suatu situs, yaitu kebiasaan beberapa user yang suka men-download di Internet. Mengambil suatu file (download) dari Internet memang menyenangkan bagi beberapa user, akan tetapi kalau tidak disiasati dengan baik hal ini justru menimbulkan masalah bagi user lainnya. Saat men-download suatu file yang besar (ex:/ file iso cd linux), biasanya bandwidth yang ada akan berkurang secara drastis, sehingga user biasa yang ingin sekadar browsing merasa begitu lambat waktu akses Internetnya. Dan kalau sudah begini, hal ini tentunya akan menurunkan produktivitas kerja.

Agar tidak terjadi hal yang demikian, maka seorang administrator harus dapat menentukan kebijakan yang berlaku pada saat user men-download suatu file dari Internet.

Sebagai contoh, penulis akan menjelaskan dengan studi kasus agar dapat lebih mudah dipahami.

Persyaratannya :

1. PT XYZ ingin agar semua komputer yang terhubung ke Internet dibatasi jumlah download-nya, yaitu ukuran file yang dapat ter-download maksimal hanya 2 MB.
2. Ketentuan No. 1, hanya berlaku selama jam kerja, yaitu dari jam 08.00–17.30, setelah lewat dari jam tersebut, user bebas men-download file dengan ukuran file tak terbatas.

Untuk menerapkan hal di atas, yang perlu Anda lakukan hanyalah menambahkan

beberapa setting-an di file squid.conf. Baca langkah-langkah di bawah ini:

1. Buka file squid.conf

```
# vi /etc/squid.conf
```

2. Lalu edit pada bagian berikut:

```
.....
.....
# Note : Untuk Settingan
Lengkapnya, dapat anda temukan
di CD InfoLinux kali ini.

# acl definisi (bagian ini
berisikan batasan-batasan
yang akan dilakukan oleh
# server squid).
acl lan src 192.168.0.0/255.
255.255.0
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 SSL_ports port 443 563
acl Safe_ports port 80 21
443 563 70 210 1025-65535
acl Safe_ports port 280
acl Safe_ports port 488
acl Safe_ports port 591
acl Safe_ports port 777
acl CONNECT method CONNECT
acl tdkbebasdownload time
08:00-17:30

# rule (bagian ini berisikan
keterangan untuk membiarkan
```

atau menolak bagian acl # yang telah dibuat).

```
http_access allow lan
http_access deny manager
http_access allow localhost
http_access deny !Safe_ports
http_access deny CONNECT
!SSL_ports
http_access deny all

acl magic_words2 url_regex
-i ftp.exe.mp3.vqf.tar.gz
.gz.tar.bz2.bz2.rpm.zip
.rar.avi.mpeg.mpe.mpg.qt
.ram.rm.raw.wav.iso

# Cancel download if file is
bigger than 2MB = 2000 X 1024
byte = 2048000 byte
reply_body_max_size
2048000 allow magic_words2
tdkbebasdownload

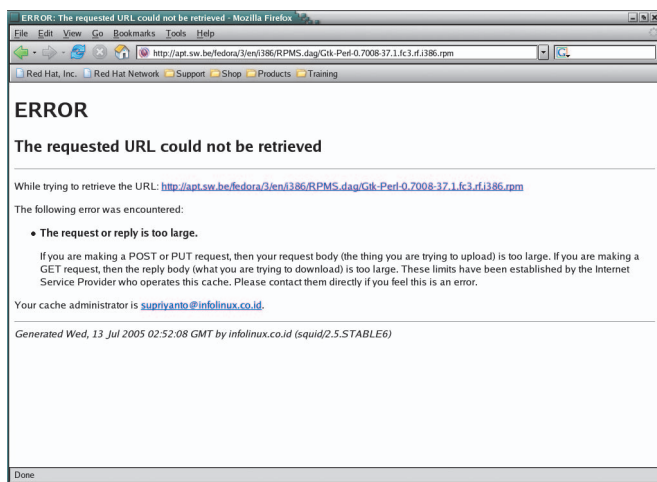
# icp access
icp_access allow lan

.....
.....
```

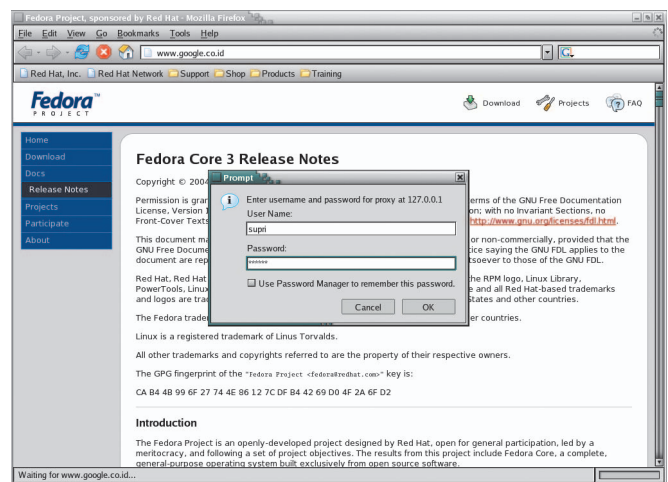
3. Restart service squid Anda, untuk melihat perubahan:

```
# service squid restart
```

4. Pada saat jam kerja, coba Anda test download suatu file dari Internet yang besar filenya lebih dari 2 MB. Jika hasil-



Peringatan file yang tidak bisa didownload karena melebihi kuota.



Metode autentikasi Squid dengan menggunakan mysql-auth.

nya adalah peringatan ERROR, maka settingan yang Anda lakukan sudah berhasil. Test juga men-download suatu file dengan ukuran kurang dari 2MB, jika dapat ter-download berarti sudah tidak ada masalah untuk pembatasan ukuran file download ini.

5. Ketika waktu jam kerja telah lewat, Test juga men-download file dengan ukuran file lebih dari 2 MB, jika hasilnya file tersebut dapat ter-download, berarti kebijakan yang telah ditentukan telah berjalan dengan baik.

6. Autentifikasi user menggunakan mysql_auth

Pada studi kasus kali ini, tidak ada hubungannya dengan studi kasus sebelumnya. Kali ini penulis akan menjelaskan metode autentifikasi user dengan menggunakan *username* dan *password* yang terdaftar di server.

Program autentifikasi yang akan penulis jelaskan bernama `mysql_auth`. Dengan `mysql_auth` ini, Anda akan lebih mudah memanajemen *username* dan *password*, karena dapat dihubungkan dengan interface yang dibuat dengan PHP maupun bahasa lainnya.

Logika program ini berjalan sebagai berikut, jika *username* dan *password* yang dimasukkan sesuai, maka program akan menghasilkan output OK, dan autentifikasi berhasil. Dan bila *username* maupun *password* tidak sesuai, maka program akan menghasilkan output ERR, dan autentifikasi akan gagal.

Kalau autentifikasi berhasil, maka user akan dapat browsing ke Internet. Tetapi jika autentifikasi gagal, user tersebut tidak dapat browsing ke Internet.

Untuk mempersingkat waktu, coba Anda ikuti penjelasan di bawah ini:

1. Download dahulu program `mysql_auth-0.8.tar.gz` dari situs http://people.arxnet.hu/airween/mysql_auth/, atau Anda dapat mencarinya pada CD majalah *InfOLINUX* edisi ini.
2. Setelah itu extract, file tersebut :

```
$ tar -xzf mysql_auth-0.8.tar.gz
```
3. Pastikan program `mysql-devel` sudah terinstal di sistem Anda, dan jangan lupa

untuk menjalankan service `mysql`.

```
# rpm -qa | grep mysql-devel
mysql-devel-3.23.58-13

# service mysqld start
```

4. Cari dan catat lokasi file `mysql.h` dan `libmysqlclient.a`

```
$ locate mysql.h
/usr/include/mysql/mysql.h

$ locate libmysqlclient.a
/usr/lib/mysql/libmysqlclient.a
```

5. Berikutnya adalah Anda harus mengedit terlebih dahulu file Makefile program `mysql_auth`.

```
$ cd mysql_auth-0.8/

$ vi Makefile
```

Edit pada bagian-bagian berikut :

- a. `CFLAGS = -I/usr/local/include -L/usr/local/lib`

menjadi

```
CFLAGS = -I/usr/include/mysql -L/usr/lib/mysql
```

- b. `$(INSTALL) -o nobody -g nogroup -m 755 mysql_auth /usr/local/squid/libexec/mysql_auth`

menjadi

```
$(INSTALL) -o squid -g squid -m 755 mysql_auth /usr/bin/mysql_auth
```

- c. `$(INSTALL) -o root -g root -m 700 mypasswd /usr/local/bin/mypasswd`

menjadi

```
$(INSTALL) -o squid -g squid -m 755 mypasswd /usr/bin/mypasswd
```

- d. `$(INSTALL) -o nobody -g nogroup -m 600 $(CONF) /usr/local/squid/etc/mysql_auth.conf`

menjadi

```
$(INSTALL) -o squid -g squid -m 600 $(CONF) /etc/mysql_auth.conf
```

- e. dan beri tanda remark (#) pada

```
$(INSTALL) -o nobody -g nogroup -m 600 $(CONF) /usr/local/squid/etc/mysql_auth.conf.default
```

menjadi

```
#$(INSTALL) -o nobody -g nogroup -m 600 $(CONF) /usr/local/squid/etc/mysql_auth.conf.default
```

6. Pindah ke directory `src`, dan edit file `define.h`

```
$ cd src/

$ vi define.h
```

Edit pada bagian-bagian berikut:

```
#define CONFIG_FILE "/usr/local/squid/etc/mysql_auth.conf"
```

menjadi

```
#define CONFIG_FILE "/etc/mysql_auth.conf"
```

7. Edit juga file `mysql_auth.conf`

```
$ vi mysql_auth.conf
```

Ubah pada bagian berikut :

- a. `mysqld_socket /tmp/mysqld.sock`

menjadi

```
mysqld_socket /var/lib/mysql/mysql.sock
```

- b. `encrypt_password_form NO`

menjadi

```
encrypt_password_form YES
```

8. Selanjutnya compile dan instal

```
$ cd mysql_auth-0.8/

$ make

$ su -c "make install"
```

9. Tambahkan database untuk autentifikasi user

```
# cd scripts/
```

```
# mysql -u root -p < create_scripts
```

10. Sekarang coba Anda tes dengan menambahkan user ke tabel data yang ada di database mysql_auth dengan menggunakan program mypasswd.

```
# mypasswd supri sup234
Password record ADDED
succesfully.
```

Anda dapat mengeceknya ke dalam tabel data yang ada di database mysql_auth, apakah record yang baru dimasukkan oleh program nypasswd, sudah ada.

```
# mysql -u root -p mysql_auth
mysql> select *from data;
+-----+-----+
| user | password |
+-----+-----+
| supri | 79d544277322393c |
+-----+-----+
1 rows in set (0.21 sec)
```

Dapat Anda lihat hasilnya di atas, kalau password yang kita masukkan untuk user supri sudah langsung terenkripsi. Hal ini karena setting-an yang terdapat di file mysql_auth.conf, di mana nilai variabel encrypt_password_form di set menjadi YES.

11. Tes validasi user dan password yang telah anda buat dengan menggunakan program mysql_auth

```
ERR
# mysql_auth
supri coba
supri sup234
OK
```

12. Setelah hasil validasi sudah benar, langkah berikutnya adalah menghubungkan program mysql_auth dengan squid. Untuk itu Anda dapat mengedit file squid.conf.

```
# vi /etc/squid.conf
.....
.....
# Tambahkan untuk autentifikasi
auth_param basic program
```

```
/usr/bin/mysql_auth
auth_param basic realm Squid
proxy-caching web server
auth_param basic children 5
auth_param basic
credentialsttl 2 hours
.....
.....
# acl definisi (bagian ini
berisikan batasan-batasan yang
akan dilakukan oleh server
# squid).
# Dan bagian ini adalah inti
dari penerapan kebijakan yang
ada di proxy server
.....
.....
acl butuhpasswd proxy_auth
REQUIRED
acl myNet src 192.168.0.0/255
.255.255.0
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
.....
.....
# rule (bagian ini berisikan
keterangan untuk membiarkan
atau menolak bagian acl
# yang telah dibuat).
.....
.....
# Baris ini juga
http_access allow butuhpasswd
http_access allow myNet
http_access allow manager
http_access allow localhost
http_access deny !Safe_ports
http_access deny CONNECT
!SSL_ports
.....
.....
# Baris ini juga
authenticate_ip_ttl 2 hours
http_access deny all
.....
.....
```

13. Test di browser, dengan mengetikkan alamat suatu situs, kemudian tekan Enter. Jika muncul layar autentifikasi setelah anda menekan tombol Enter, coba Anda

masukkan username dan password yang telah dibuat, sebagai contoh : username : supri, password: sup234.

Jika masuk dan tidak mengalami masalah, berarti metode autentifikasinya sudah berjalan dengan baik.

7. Transparant proxy

Setelah menjelaskan keenam cara di atas, akhirnya sampai juga pada cara terakhir yang akan penulis jelaskan. Pada semua kasus sebelumnya, Anda harus men-setting secara manual setting-an proxy di web browser client agar dapat ber-Internet. Mungkin kalau hanya sepuluh client, hal itu tidak menjadi masalah. Tetapi bagaimana jika komputer yang harus disetting berjumlah ratusan, tentu hal ini akan merepotkan Anda sebagai administrator. Belum lagi jika suatu saat, terdapat lagi perubahan IP dan port proxy server yang digunakan.

Untuk menyiasati hal tersebut, diperlukan suatu cara agar Anda tidak perlu memasukkan secara manual setting-an proxy server yang berlaku. Caranya adalah Anda dapat menggunakan transparant proxy. Prinsip kerja transparant proxy adalah sebuah firewall atau redirector lainnya akan menangkap koneksi TCP yang ditujukan ke port tertentu pada remote host, dan kemudian akan mengarahkan koneksi TCP tersebut ke proxy server lokal. Proxy server menggunakan header HTTP untuk menentukan ke mana proxy akan melakukan koneksi dan request dari mana yang akan di-proxy. Untuk mengaplikasikan transparant proxy, Anda dapat memerlukan aplikasi Iptables. Dengan Iptables, anda cukup membuat rule untuk menangkap trafik yang ditujukan untuk port 80, dan mengarahkan trafik ini ke port dari proxy server (biasanya 3128 atau 8080).

Untuk lebih jelasnya, Anda dapat mengikuti petunjuk yang diberikan ada di bawah ini:

1. Dimisalkan kali ini Anda sudah dapat menjalankan proxy server secara manual dengan baik, sekarang tinggal bagaimana caranya agar dapat berjalan secara transparant proxy.
2. Pastikan paket dan service iptables sudah terinstal dengan baik di sistem Anda.
3. Squid terkonfigurasi dengan menggunakan port 3128.

4. Alamat network yang digunakan adalah 192.168.0.0/24.

Cara mengatur konfigurasi transparant proxy:

1. Pastikan kalau sistem telah mendukung IP Forwarding. Caranya ubah parameter yang ada di /etc/sysctl.conf pada bagian ip_forward.

```
net.ipv4.ip_forward = 0
```

menjadi:

```
net.ipv4.ip_forward = 1
```

Setelah itu, restart service network Anda:

```
# service network restart
```

2. Berikutnya edit file squid.conf Anda, kemudian tambahkan baris di bawah ini pada bagian paling bawah dari file itu.

```
# transparent proxy
httpd_accel_host virtual
httpd_accel_port 80
httpd_accel_with_proxy on
httpd_accel_uses_host_header on
```

3. Lakukan masquerading dengan menggunakan iptables. IP masquerading berguna untuk menghubungkan beberapa komputer yang terkoneksi ke sebuah komputer yang sudah terkoneksi ke Internet agar dapat mengakses ke Internet, atau istilahnya *Internet Connection Sharing*.

```
iptables -A POSTROUTING
-j MASQUERADE -t nat -s
192.168.0.0/24 -o eth0
```

Option -o tersebut tolong anda sesuaikan dengan interface yang terdekat dengan jaringan luar.

4. Selanjutnya arahkan semua permintaan web pada port 80 ke port squid. Untuk kondisi ini, terdapat dua buah opsi. Jika squid dan firewall yang mengarahkan berada pada satu komputer, gunakan perintah ini:

```
iptables -t nat -p tcp -A
PREROUTING -s 192.168.0.0/24
-d 0/0 -dport 80 -j REDIRECT
-to-ports 3128
```

Jika Squid dan firewall yang mengarahkan tidak berada pada satu komputer.

Misal Squid berada pada komputer yang ber-IP 192.168.0.4 dan port yang digunakan adalah 3128 atau kita sebut saja komputer ini dengan nama squid-box. Dan satunya lagi komputer yang terhubung ke Internet langsung sebagai firewall mempunyai IP 192.168.0.1 kita sebut saja komputer ini dengan nama iptables-box. Dari komputer iptables-box, coba Anda ketikkan perintah berikut untuk mengaktifkan transparant proxy di mesin squid-box.

```
iptables -t nat -A PREROUTING
-i eth0 -s ! 192.168.0.4 -p
tcp --dport 80 -j DNAT
--to 192.168.0.4:3128
```

```
iptables -t nat -A POSTROUTING
-o eth0 -s 192.168.0.0/24
-d 192.168.0.4 -j SNAT
-to 192.168.0.1
```

```
iptables -A FORWARD -s
192.168.0.0/24 -d 192.168.0.4
-i eth0 -o eth0 -p tcp --
dport 3128 -j ACCEPT
```

Setelah itu, coba amati file access.log di mesin proxy Anda. Jika semuanya sudah benar, seharusnya jika ada user yang sedang mengakses web, Anda sudah dapat mengamati prosesnya dari mesin proxy tersebut.

Demikian artikel tentang *step by step* konfigurasi Squid. Sebenarnya masih banyak lagi fungsi Squid lainnya yang dapat anda telusuri lebih lanjut di file konfigurasi Squid.conf. Pada artikel ini, penulis sudah menjelaskan secara garis besar konfigurasi Squid yang sering digunakan oleh sebagian besar administrator.

Namun pada intinya, sesuaikan saja dengan kebijakan yang benar-benar dibutuhkan oleh Anda. Terkadang tidak semua fungsi yang ada benar-benar dibutuhkan di dalam suatu jaringan.

Akhir kata, semoga dengan artikel singkat ini, Anda dapat membuat proxy server yang andal tanpa terbentur masalah harga lisensi software proxy komersial yang mahal. Indahnya dunia open source! 🙏

Supriyanto (supriyanto@infolinux.co.id)

MORE SPACE RELIABILITY & TIME & MONEY

LINUX and FreeBSD

Features :

- Unlimited data transfer
- Complete control panels
- POP3 email, FTP access
- SSH, CGI, SQL.
- and much more...
- Start from Rp. 19.500,-/ month
- Free Setup *)
- 2 Months Free **)

Server Hosting

Features :

- Location NOC Jakarta - Indonesia (IIX)
- Size server : 1 U Rackmount
- Bandwidth : 128 kbps
- IP Address : 8 (max)
- Colocation : Rp. 1.000.000,-/ month

ALSO

- Colocation & Dedicated Server in USA
- Domain Name Register
- Benefit Reseller Program

*"IT'S NEVER BEEN EASIER
TO TAKE YOUR BUSINESS ONLINE"*

Note : *) Transfer (restriction apply)
**) 1 year payment

CAKRAWEB
Supporting You to a Web Success

Cyber Building (d/h Elektrindo) 10 th Floor
Jl. Kuningan Barat No. 8 Jakarta Selatan 12710
Phone. (021) 526 8000 Fax. (021) 52 66 444
<http://www.cakraweb.com> - info@cakraweb.com