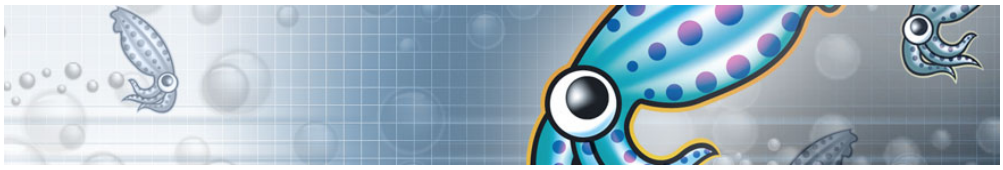


SQUID PROXY

WEBFILTER

Daftar Isi

Proxy *Overview*

1. Pengertian Proxy

Secara terminologi istilah **proxy** dapat diartikan sebagai seseorang/lembaga yang bertindak sebagai perantara atau atas nama dari orang lain/lembaga dalam suatu hal.

Namun dalam dunia jaringan komputer, istilah **proxy** berarti komputer yang berfungsi sebagai perantara antara *client* dan server dalam jaringan komputer.

2. Fungsi Proxy

Proxy memiliki 3 fungsi utama, yaitu:

a. Firewall

Proxy bekerja pada layer aplikasi (dalam OSI Layer), maka filtering yang dilakukan oleh proxy lebih "cerdas" daripada firewall biasa. Proxy web server dapat mengecek URL dari *outgoing request* (permintaan akses keluar) untuk halaman web. Dengan kemampuan ini, administrator dapat melarang atau mengizinkan akses ke domain tertentu. Firewall biasa tidak dapat melihat nama domain di dalam pesan tersebut, karena firewall hanya memeriksa header paket data.

b. *Gateway*

Untuk dapat mengakses internet, sebuah komputer harus memiliki sebuah IP *public*. Untuk dapat mengakses internet secara bersama-sama dengan menggunakan satu IP *public*, dibutuhkan sebuah komputer yang memiliki IP *public*, yang digunakan sebagai *gateway* komputer-komputer lain. Dalam hal ini, proxy server juga berfungsi sebagai *gateway*. Server ini mempunyai dua *interface*, untuk koneksi ke internet dan untuk koneksi ke jaringan lokal.

c. *Cache*

Fungsi proxy server yang lain adalah untuk web *caching*. *Caching* di sini diartikan sebagai penyimpanan internet *object* (gambar/halaman web) dari suatu website yang sudah pernah diakses, sehingga bila akan mengakses objek yang sama di internet, tidak perlu mengambil dari internet, tetapi cukup dari proxy karena sudah disimpan. Bandwidth yang dipakai pun akan lebih hemat, dan dapat mempercepat akses ke website.

Squid Proxy *Overview*

Squid adalah aplikasi untuk proxy yang berjalan di lingkungan sistem operasi *.nix. Namun, dalam perkembangannya ada pula squid yang berjalan di lingkungan sistem operasi Windows.

Konfigurasi Squid

File konfigurasi untuk squid adalah **squid.conf** yang terletak pada direktori /etc/squid/squid.conf. Beberapa konfigurasi penting dari squid.conf adalah:

- **http_port**
  Mendefinisikan port yang digunakan untuk koneksi dengan *client*. Defaultnya adalah 3128.
- **icp_port**
  Mendefinisikan port yang digunakan untuk koneksi dengan proxy lain.
- **cache_mem**
  Menentukan besar memori yang digunakan untuk menyimpan objek yang pernah di-download.
- **cache_dir**
  Menentukan direktori penyimpanan objek yang disimpan.
- **http_access**
  Menunjuk alamat-alamat yang diperbolehkan atau tidak untuk mengakses proxy.
- **cache_mgr**
  Alamat Email yang di tampilkan bila proxy tidak dapat menampilkan halaman web yang diminta.
- **visible_hostname**
  Informasi di *footer* bila proxy tidak dapat menampilkan halaman web yang diminta.

Building Squid Proxy

1. Spesifikasi Sistem

Spesifikasi dari sistem yang digunakan adalah sebagai berikut :

1. 1 PC
2. Sistem Operasi Ubuntu 9.04 Desktop Jaunty Jackalope
3. 2 NIC dengan 2 IP
   - IP ke internet : 192.168.221.129
   - IP ke jaringan lokal : 192.168.1.1
4. Squid versi 2.7 STABLE3

2. Instalasi Squid

Berikut merupakan langkah-langkah instalasi squid di Ubuntu :

a. Periksa apakah squid sudah terinstal atau belum.

```
# dpkg -l | grep squid
```

b. Jika belum, install squid melalui apt-get.

```
# apt-get install squid
```

3. Konfigurasi squid.conf

Berikut merupakan langkah-langkah konfigurasi squid di Ubuntu :

a. Buka file squid.conf dengan teks editor.

```
# pico /etc/squid/squid.conf
```

b. Lakukan konfigurasi berikut dan simpan.

```
http_port 3128
icp_port 3130
udp_incoming_address 0.0.0.0
udp_outgoing_address 255.255.255.255
hierarchy_stoplist cgi-bin ?
acl QUERY urlpath_regex cgi-bin \?
no_cache deny QUERY
cache_mem 8 MB
maximum_object_size 4096 KB
cache_dir ufs /var/spool/squid 100 16 256
cache access log /var/log/squid/access.log
```

```
cache_log /var/log/squid/cache.log
auth_param basic children 5
auth_param basic realm Squid proxy-caching web server
auth_param basic credentialsttl 2 hours
refresh_pattern ^ftp: 1440 20% 10080
refresh_pattern ^gopher: 1440 0% 1440
refresh_pattern . 0 20% 4320
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 443 563
acl Safe_ports port 80
acl Safe_ports port 21
acl Safe_ports port 443 563
acl Safe_ports port 70
acl Safe_ports port 210
acl Safe_ports port 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
http_access allow manager localhost
http_access deny manager
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost
http_access allow all
http_reply_access allow all
icp_access allow all
cache_mgr webmaster
cache_effective_user proxy
cache_effective_group proxy
visible_hostname datacomm.co.id
memory_pools on
log_icp_queries on
coredump_dir /var/spool/squid
```

c. Buat direktori *cache*

```
# squid -z
```

atau :

```
# /usr/sbin/squid -z
```

4. Administrasi *Service*

a. Menjalankan squid agar aktif.

```
# /etc/init.d/squid start
```

b. Jika mengubah konfigurasi squid, maka restart daemon squid agar squid membaca ulang konfigurasi yang sudah dibuat.

```
# /etc/init.d/squid restart
```

atau :

```
# squid –k reconfigure
```

c. Menghentikan squid.

```
# /etc/init.d/squid stop
```

Konfigurasi *Client*

1. Konfigurasi IP *Address*

Setting IP *address* pada *client* agar satu jaringan dengan IP *address* lokal dari proxy server (192.168.1.1). Contohnya, IP *address client* diset menjadi 192.168.1.2.

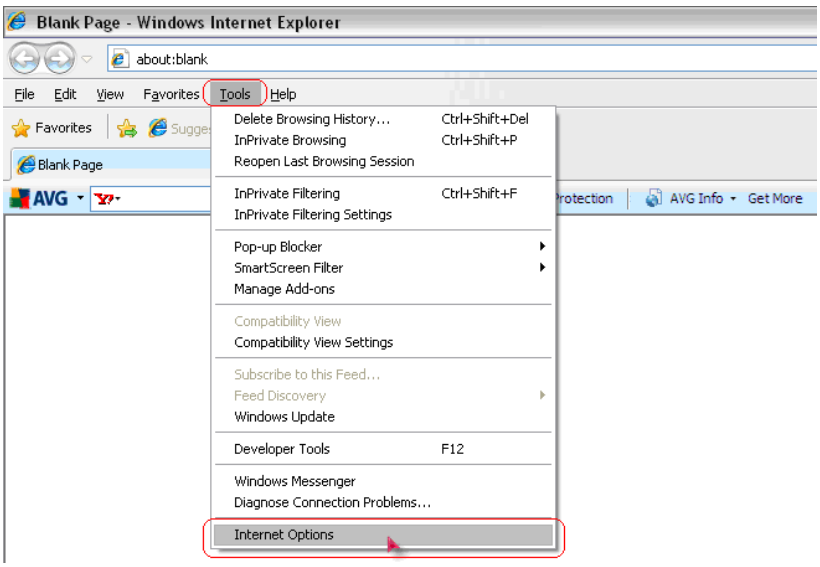
Setting sebagai berikut :

IP *address*	: 192.168.1.2
Netmask	: 255.255.255.0
Default gateway	: 192.168.1.1

2. Konfigurasi Browser

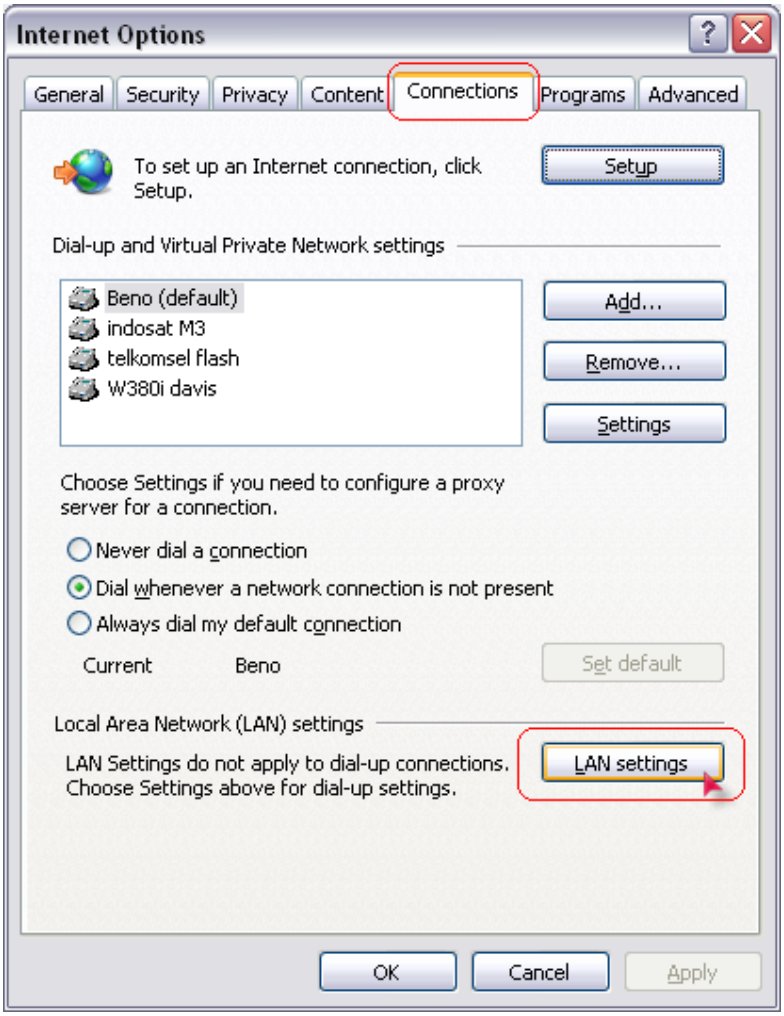
a. Konfigurasi di Windows

- Internet Explorer (IE)
  - Pilih menu **Tools** kemudian pilih **Internet Options**.



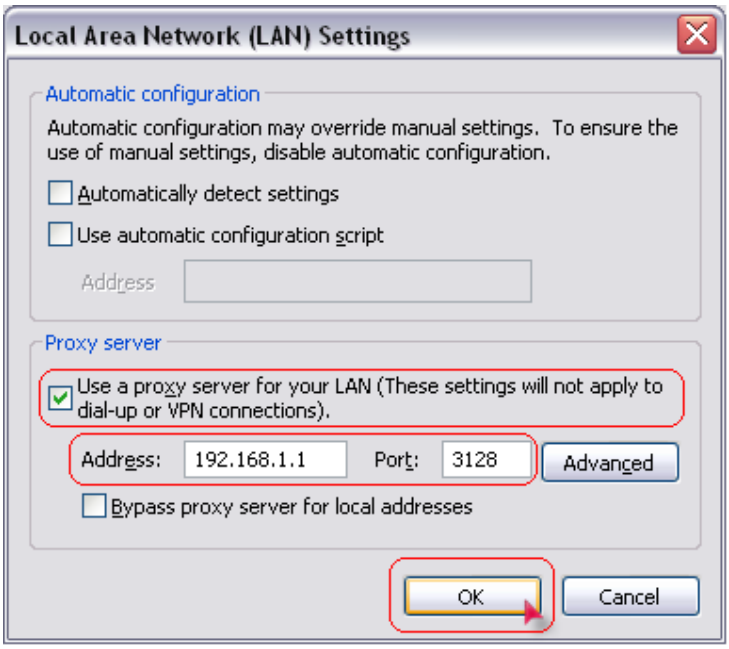
Gambar 4.1 Menu Tools IE

- Pilih tab **Connections** kemudian klik tombol **LAN settings**.



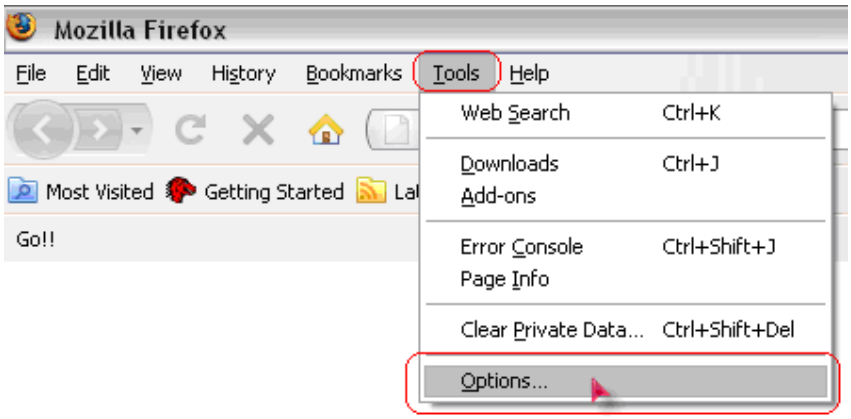
Gambar 4.2 Internet Options → Connections → LAN settings

- *Check* opsi **Use a proxy server** pada bagian bawah, lalu isikan alamat IP dari proxy yaitu **192.168.1.1** dan port proxy yang digunakan yaitu **3128**. Klik **OK**.



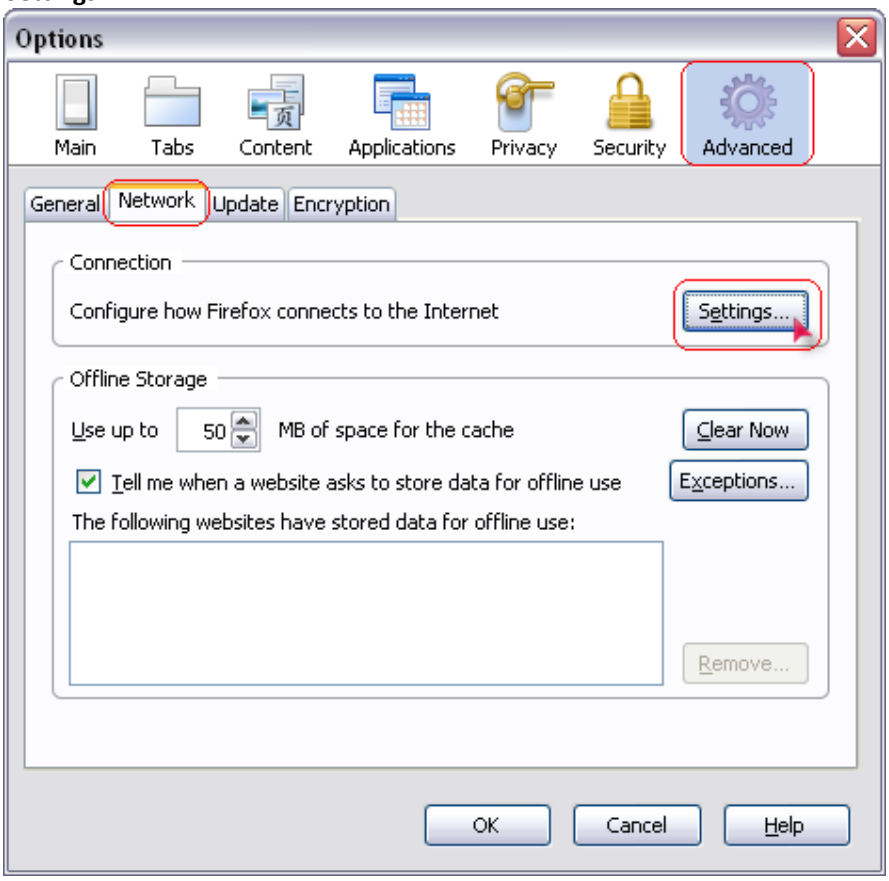
Gambar 4.3 LAN settings

- Mozilla Firefox
  - Pilih menu **Tools** kemudian pilih **Options**.



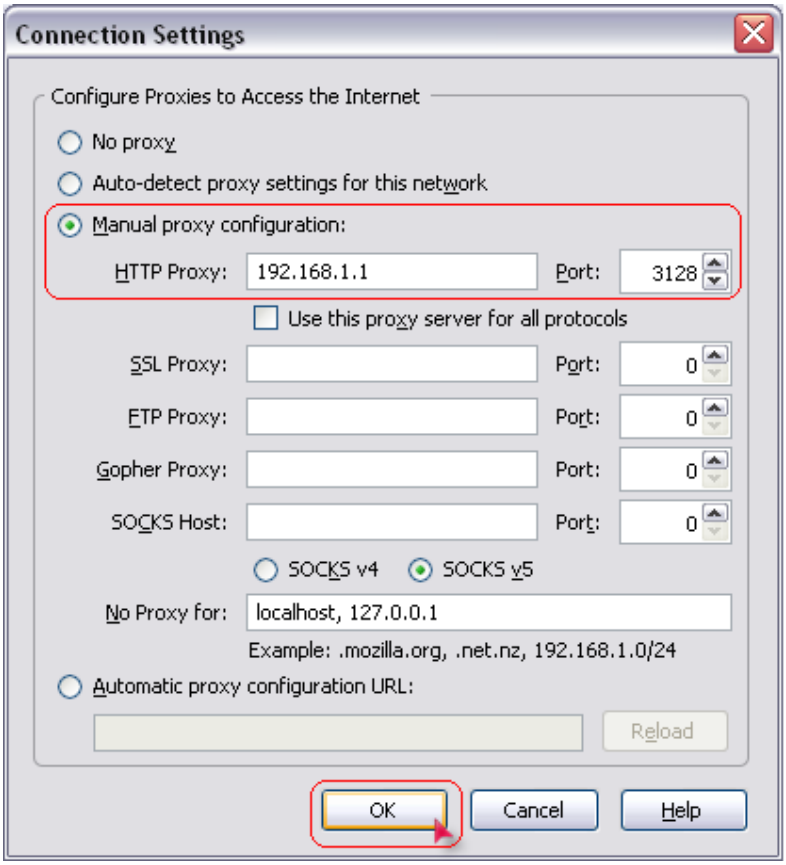
Gambar 4.4 Menu Tools Mozilla Firefox

- Pilih tombol **Advanced** kemudian pilih tab **Network**, dan klik tombol **Settings**.



Gambar 4.5 Options → Advanced → Network → Settings

- Pilih opsi **Manual proxy configuration** pada bagian bawah, lalu isikan alamat IP dari proxy yaitu **192.168.1.1** dan port proxy yang digunakan yaitu **3128**. Klik **OK**.



Gambar 4.6 Connection Settings

b. Konfigurasi di Linux (Mozilla Firefox)

- Buka Mozilla Firefox.
- Pilih menu **Edit → Preferences → Advanced → Proxies**.
- Isikan alamat IP dari proxy yaitu **192.168.1.1** dan port proxy yang digunakan yaitu **3128**. Klik **OK**.

Webfiltering

Squid dapat digunakan untuk memfilter halaman-halaman web yang boleh diakses dan yang tidak boleh diakses.

1. Squid Proxy Webfiltering

Berikut merupakan langkah-langkah konfigurasi squid untuk webfiltering.

a. Buat file "blok.txt" dengan teks editor.

```
# pico /etc/squid/blok.txt
```

b. Isi dengan domain ataupun kata-kata (string) yang ingin diblok agar user tidak dapat mengakses halaman web yang didaftarkan dalam file. Setelah selesai, simpan file ini.

```
klasiber
```

c. Edit file squid.conf, tambah baris berikut pada bagian acl dan http_access.

```
acl blok url_regex -i "/etc/squid/blok.txt"
acl coba dstdomain uii.ac.id
http_access deny blok
http_access deny coba
http_access allow all
```

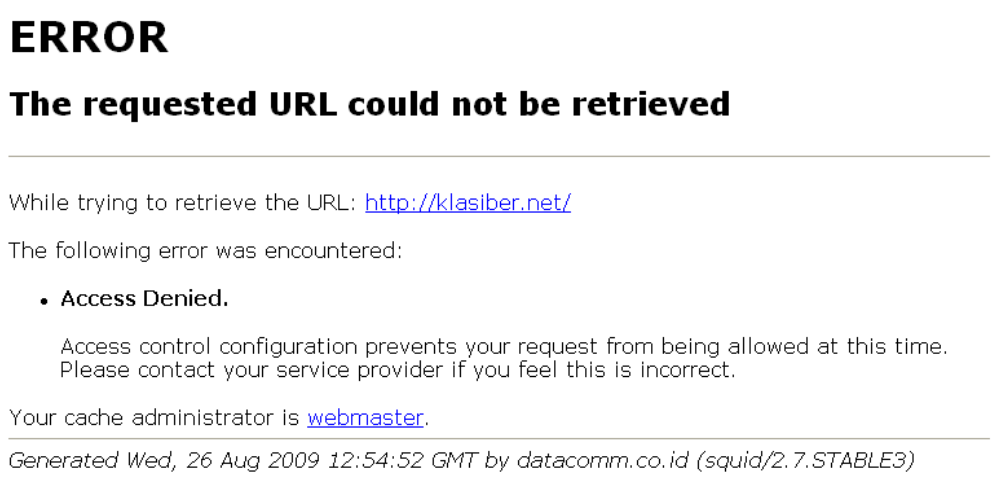
Maksud dari konfigurasi tersebut adalah membuat aturan pengaksesan situs pada direktif **acl** (*access control list*) yang didefinisikan di dalam file /etc/squid/blok.txt (situs yang mengandung string **klasiber**) dengan parameter **url_regex –i**. Dan juga membuat aturan pengaksesan situs yang didefinisikan dengan parameter **dstdomain**. Untuk parameter **dstdomain** harus disertai nama situs secara lengkap.

Untuk memblok situs-situs tersebut, pendefinisian dilakukan pada direktif **http_access**. Setting http_access sebagai **deny** jika situs yang dimaksud tidak boleh diakses. Dan setting sebagai **allow** jika situs yang dimaksud boleh diakses. Kemudian diikuti nama dari acl.

d. Rekonfigurasi squid dengan perintah berikut.

```
# squid –k reconfigure
```

e. Dengan konfigurasi tersebut, ketika user jaringan lokal mengakses situs **klasiber.net** (mengandung string **klasiber**), maka akan muncul halaman peringatan sebagai berikut.



Gambar 5.1 Halaman error Access Denied

2. Kustomisasi Halaman Error Access Denied

Halaman error Access Denied akan muncul apabila user tidak dapat mengakses situs yang telah diblok. Halaman ini dapat dikustomisasi. File-nya terletak di /usr/share/squid/errors/English/ERR_ACCESS_DENIED.

Berikut langkah-langkah mengkustomisasi halaman error Access Denied.

a. Edit file /usr/share/squid/errors/English/ERR_ACCESS_DENIED dengan teks editor.

```
# pico /usr/share/squid/errors/English/ERR_ACCESS_DENIED
```

b. Misal mengganti tulisan **Access Denied** menjadi **Maaf, Anda tidak diperkenankan mengakses halaman ini. Terima kasih.** Kemudian simpan file ini.

c. Restart squid dengan perintah berikut.

```
# /etc/init.d/squid restart
```

d. Akses kembali situs klasiber.net,maka akan muncul halaman error Access denied yang telah dikustomisasi seperti berikut.

Gambar 5.2 Halaman error Access Denied yang telah dikustomisasi

SARG

(*Squid Analysis Report Generator*)

Untuk melihat halaman-halaman yang pernah dibuka oleh user jaringan lokal yang terkoneksi ke proxy server, dapat digunakan utilitas yang bernama SARG (*Squid Analysis Report Generator*). Mengenai SARG, dapat dilihat infonya melalui situs http://sarg.sourceforge.net/sarg.php.

1. Instalasi SARG dan Apache2

Lakukan instalasi SARG dan Apache2 melalui apt-get. Paket apache2 dibutuhkan sebagai web server, di mana nanti analisis menggunakan SARG diakses melalui halaman web.

```
# apt-get install sarg apache2
```

2. Konfigurasi SARG

a. Edit file /etc/sarg/sarg.conf dengan teks editor.

```
# pico /etc/sarg/sarg.conf
```

b. Lakukan konfigurasi seperti berikut dan simpan.

```
language English
access_log /var/log/squid/acces.log
graphs yes
graph_days_bytes_bar_color orange
title "Squid User Access Reports"
output_dir /var/www/squid-reports
resolve_ip no
topuser_sort_field BYTES reverse
user_sort_field BYTES reverse
lastlog 3
remove_temp_files yes
index yes
index_tree file
overwrite_report yes
topsites_num 200
topsites_sort_order CONNECT D
index_sort_order D
```

```
report_type topusers topsites sites_users users_sites
date_time denied auth_failures site_user_time_date
downloads
show_successful_message yes
show_read_statistics yes
topuser_fields NUM DATE_TIME USERID CONNECT BYTES
%BYTES IN-CACHE-OUT USED_TIME MILISEC %TIME TOTAL
AVERAGE
topuser_num 0
```

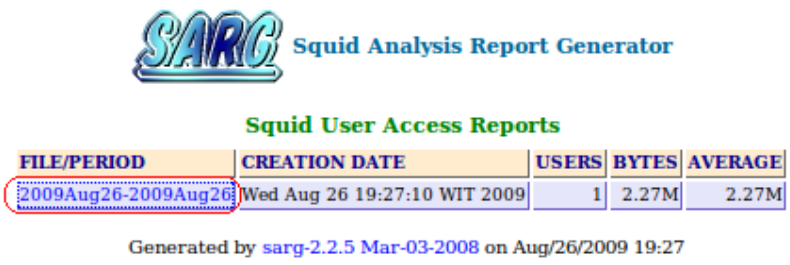
3. Menjalankan SARG

Jalankan SARG dengan cara berikut.

```
/usr/bin/sarg -l /var/log/squid/access.log
```

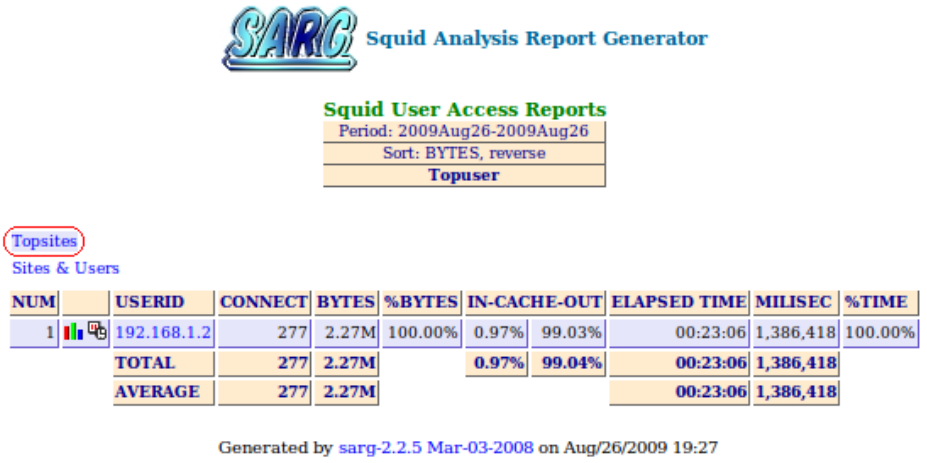
4. Analisis dengan SARG

a. Buka browser dan arahkan ke http://[IP proxy server]/squid-reports, yaitu http://192.168.1.1/squid-reports. Maka akan muncul halaman seperti berikut. Perhatikan bagian **File/Period**. Klik pada tanggal di bagian **File/Period** untuk meihat detail analisis.



Gambar 6.1 Halaman depan SARG

b. Detail analisis dapat dilihat berdasarkan menu **Topsites** dan **Sites & Users**. Klik pada menu **Topsites**.



Squid Analysis Report Generator

Squid User Access Reports

Period: 2009Aug26-2009Aug26

Sort: BYTES, reverse

Topuser

Topsites

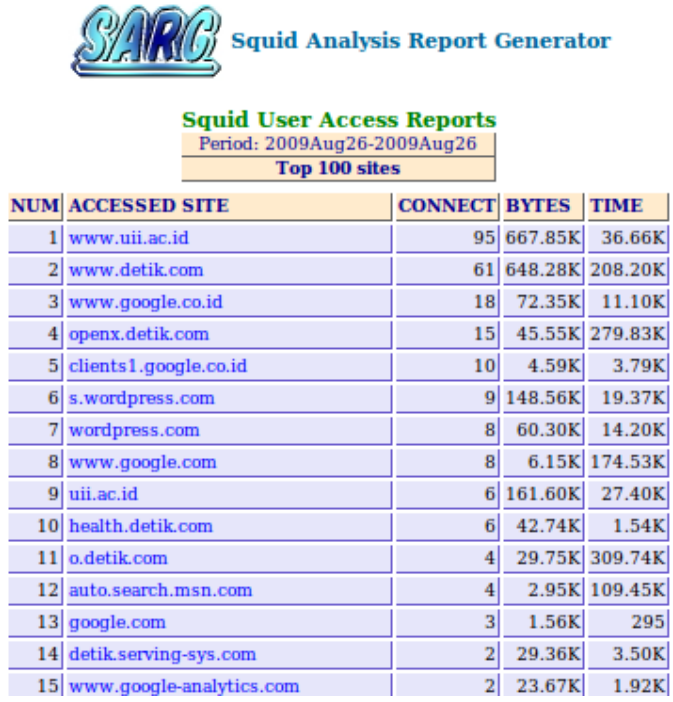
Sites & Users

NUM		USERID	CONNECT	BYTES	%BYTES	IN-CACHE-OUT		ELAPSED TIME	MILISEC	%TIME
1		192.168.1.2	277	2.27M	100.00%	0.97%	99.03%	00:23:06	1,386,418	100.00%
		TOTAL	**277**	**2.27M**		**0.97%**	**99.04%**	**00:23:06**	**1,386,418**	
		AVERAGE	**277**	**2.27M**				**00:23:06**	**1,386,418**	

Generated by sarg-2.2.5 Mar-03-2008 on Aug/26/2009 19:27

Gambar 6.2 Menu Topsites

c. Berikut muncul analisis mengenai peringkat teratas halaman web yang sering diakses oleh user. Untuk kembali ke halaman sebelumnya, klik tombol *back* pada browser.



Squid Analysis Report Generator

Squid User Access Reports

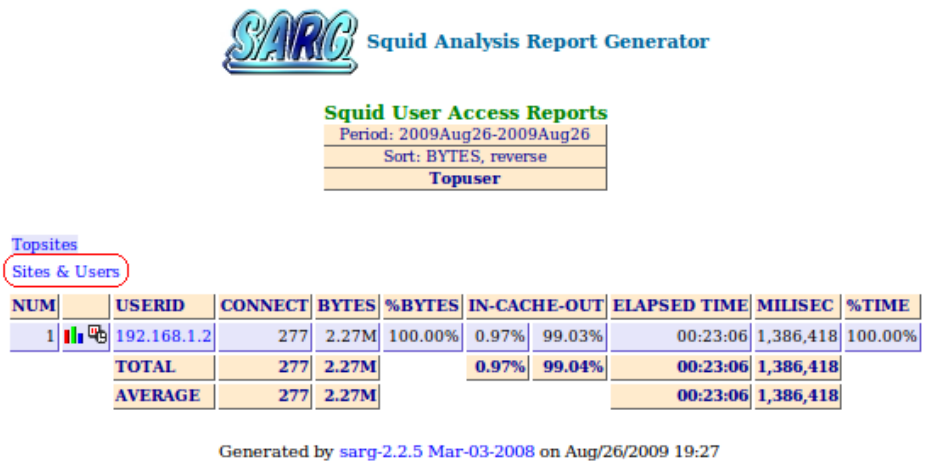
Period: 2009Aug26-2009Aug26

Top 100 sites

NUM	ACCESSED SITE	CONNECT	BYTES	TIME
1	www.uii.ac.id	95	667.85K	36.66K
2	www.detik.com	61	648.28K	208.20K
3	www.google.co.id	18	72.35K	11.10K
4	openx.detik.com	15	45.55K	279.83K
5	clients1.google.co.id	10	4.59K	3.79K
6	s.wordpress.com	9	148.56K	19.37K
7	wordpress.com	8	60.30K	14.20K
8	www.google.com	8	6.15K	174.53K
9	uii.ac.id	6	161.60K	27.40K
10	health.detik.com	6	42.74K	1.54K
11	o.detik.com	4	29.75K	309.74K
12	auto.search.msn.com	4	2.95K	109.45K
13	google.com	3	1.56K	295
14	detik.serving-sys.com	2	29.36K	3.50K
15	www.google-analytics.com	2	23.67K	1.92K

Gambar 6.3 Analisis Topsites

d. Klik pada menu **Sites & Users**.



Squid Analysis Report Generator

Squid User Access Reports
Period: 2009Aug26-2009Aug26
Sort: BYTES, reverse
Topuser

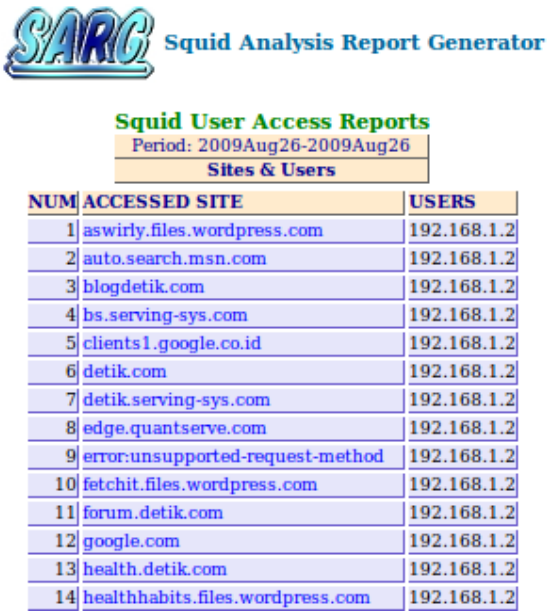
Topsites
Sites & Users

NUM		USERID	CONNECT	BYTES	%BYTES	IN-CACHE-OUT		ELAPSED TIME	MILISEC	%TIME
1		192.168.1.2	277	2.27M	100.00%	0.97%	99.03%	00:23:06	1,386,418	100.00%
		TOTAL	277	2.27M		0.97%	99.04%	00:23:06	1,386,418	
		AVERAGE	277	2.27M				00:23:06	1,386,418	

Generated by sarg-2.2.5 Mar-03-2008 on Aug/26/2009 19:27

Gambar 6.3 Menu Sites & Users

e. Berikut muncul analisis mengenai siapa yang mengakses situs apa. Untuk kembali ke halaman sebelumnya, klik tombol *back* pada browser.



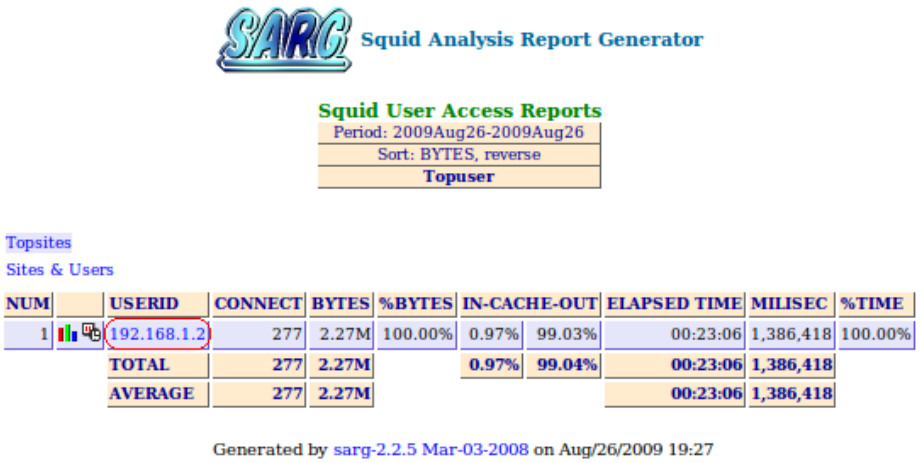
Squid Analysis Report Generator

Squid User Access Reports
Period: 2009Aug26-2009Aug26
Sites & Users

NUM	ACCESSED SITE	USERS
1	aswirly.files.wordpress.com	192.168.1.2
2	auto.search.msn.com	192.168.1.2
3	blogdetik.com	192.168.1.2
4	bs.serving-sys.com	192.168.1.2
5	clients1.google.co.id	192.168.1.2
6	detik.com	192.168.1.2
7	detik.serving-sys.com	192.168.1.2
8	edge.quantserve.com	192.168.1.2
9	error:unsupported-request-method	192.168.1.2
10	fetchit.files.wordpress.com	192.168.1.2
11	forum.detik.com	192.168.1.2
12	google.com	192.168.1.2
13	health.detik.com	192.168.1.2
14	healthhabits.files.wordpress.com	192.168.1.2

Gambar 6.4 Analisis Sites & Users

f. Klik pada IP *address* user yang akses ke web melalui proxy.



Squid Analysis Report Generator

Squid User Access Reports
Period: 2009Aug26-2009Aug26
Sort: BYTES, reverse
Topuser

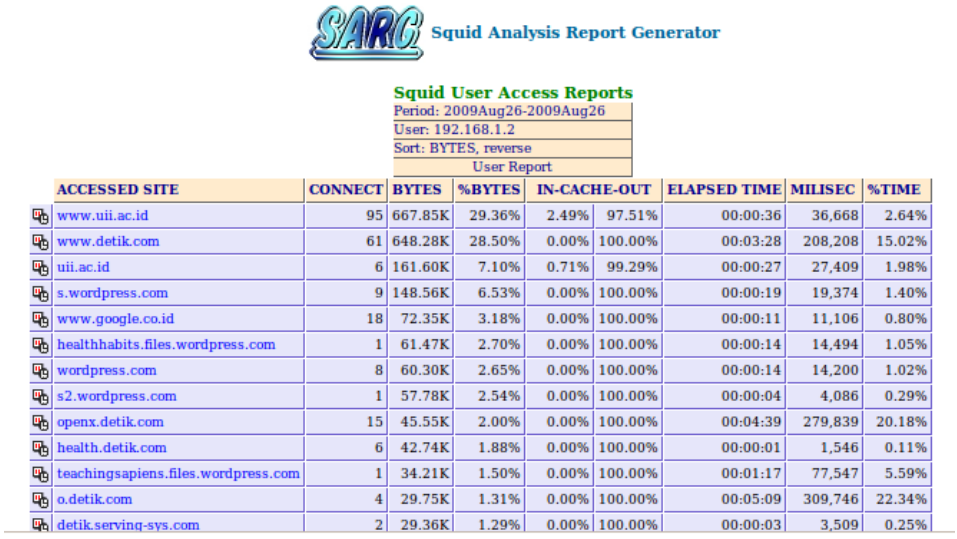
Topsites
Sites & Users

NUM		USERID	CONNECT	BYTES	%BYTES	IN-CACHE-OUT		ELAPSED TIME	MILISEC	%TIME
1		192.168.1.2	277	2.27M	100.00%	0.97%	99.03%	00:23:06	1,386,418	100.00%
		TOTAL	277	2.27M		0.97%	99.04%	00:23:06	1,386,418	
		AVERAGE	277	2.27M				00:23:06	1,386,418	

Generated by sarg-2.2.5 Mar-03-2008 on Aug/26/2009 19:27

Gambar 6.5 IP *address* user

g. Berikut muncul analisis mengenai situs apa saja yang diakses oleh user tertentu. Untuk kembali ke halaman sebelumnya, klik tombol *back* pada browser.



Squid Analysis Report Generator

Squid User Access Reports
Period: 2009Aug26-2009Aug26
User: 192.168.1.2
Sort: BYTES, reverse
User Report

ACCESSED SITE	CONNECT	BYTES	%BYTES	IN-CACHE-OUT		ELAPSED TIME	MILISEC	%TIME
www.uii.ac.id	95	667.85K	29.36%	2.49%	97.51%	00:00:36	36,668	2.64%
www.detik.com	61	648.28K	28.50%	0.00%	100.00%	00:03:28	208,208	15.02%
uii.ac.id	6	161.60K	7.10%	0.71%	99.29%	00:00:27	27,409	1.98%
s.wordpress.com	9	148.56K	6.53%	0.00%	100.00%	00:00:19	19,374	1.40%
www.google.co.id	18	72.35K	3.18%	0.00%	100.00%	00:00:11	11,106	0.80%
healthhabits.files.wordpress.com	1	61.47K	2.70%	0.00%	100.00%	00:00:14	14,494	1.05%
wordpress.com	8	60.30K	2.65%	0.00%	100.00%	00:00:14	14,200	1.02%
s2.wordpress.com	1	57.78K	2.54%	0.00%	100.00%	00:00:04	4,086	0.29%
openx.detik.com	15	45.55K	2.00%	0.00%	100.00%	00:04:39	279,839	20.18%
health.detik.com	6	42.74K	1.88%	0.00%	100.00%	00:00:01	1,546	0.11%
teachingsapiens.files.wordpress.com	1	34.21K	1.50%	0.00%	100.00%	00:01:17	77,547	5.59%
o.detik.com	4	29.75K	1.31%	0.00%	100.00%	00:05:09	309,746	22.34%
detik.serving-sys.com	2	29.36K	1.29%	0.00%	100.00%	00:00:03	3,509	0.25%

Gambar 6.6 Analisis situs yang diakses oleh user tertentu

Transparent Proxy

Kelemahan dari proxy yang konvensional adalah masih harus men-setting di browser yang digunakan oleh user. Apabila user yang ada di jaringan sangat banyak, maka hal ini akan menjadi sesuatu yang merepotkan.

Oleh karena itu, maka digunakanlah suatu metode di mana user dipaksa menggunakan proxy tanpa tahu kalau user tersebut mengakses halaman web melalui proxy. Metode ini disebut ***Transparent Proxy***.

Berikut langkah-langkah yang dilakukan untuk setting *transparent proxy*.

1. Edit file /etc/squid/squid.conf pada bagian http_port. Kemudian simpan.

```
http_port 3128 transparent
```

2. Restart squid.

```
# /etc/init.d/squid restart
```

3. Buat aturan di firewall dengan script berikut. Gunakan teks editor.

```
# pico /etc/squid/maketransparentproxy.sh
```

```
#!/bin/sh
# Squid server IP
      SQUID_SERVER="192.168.1.1"
# Interface connected to Internet
      INTERNET="eth0"
# Address connected to LAN
      LOCAL="192.168.1.0/24"
# Squid port
      SQUID_PORT="3128"
# Clean old firewall
      iptables -F
      iptables -X
      iptables -t nat -F
      iptables -t nat -X
      iptables -t mangle -F
      iptables -t mangle -X
# Enable forwarding
            echo 1 > /proc/sys/net/ipv4/ip_forward
```

```
# Setting default filter policy
      iptables –P INPUT DROP
      iptables –P OUTPUT ACCEPT
# Unlimited access to loop back
      iptables –A INPUT –i lo –j ACCEPT
      iptables –A OUTPUT –o lo –j ACCEPT
# Allow UDP, DNS, and Passive FTP
      iptables –A INPUT –i $INTERNET –m state --state
      ESTABLISHED,RELATED –j ACCEPT
# Set this system as a router for Rest of LAN
      iptables –t nat –A POSTROUTING –o $INTERNET –j
      MASQUERADE
      iptables –A FORWARD –s $LOCAL –j ACCEPT
# Unlimited access to LAN
      iptables –A INPUT –s $LOCAL –j ACCEPT
      iptables –A FORWARD –s $LOCAL –j ACCEPT
# DNAT port 80 request coming from LAN systems to squid 3128
($SQUID_PORT) aka transparent proxy
      iptables –t nat –A PREROUTING –s $LOCAL –p tcp
      --dport 80 –j DNAT --to $SQUID_SERVER:$SQUID_PORT
# If it is same system
      iptables –t nat –A PREROUTING –i $INTERNET –p tcp
      --dport 80 –j REDIRECT --to-port $SQUID_PORT
# DROP everything and log it
      iptables –A INPUT –j LOG
      iptables –A INPUT –j DROP
```

4. Jalankan script firewall.

```
# chmod +x /etc/ squid/maketransparentproxy.sh

# /etc/squid/maketransparentproxy.sh
```

5. Setting gateway user/*client* menggunakan IP local Squid. User dapat mengakses halaman web tanpa harus di-setting browsernya terlebih dahulu.