

Squid Proxy Server

Workshop Administrasi Jaringan

Praktikum ke 6



Albi Nur Rosif
3122522010
D3 IT PSDKU-SM

**PRODI D3 TEKNIK INFORMATIKA
DEPARTEMEN TEKNIK INFORMATIKA DAN KOMPUTER
PENS PSDKU SUMENEP**

1. Squid Proxy Server

1. Server : Install & Konfigurasi Squid

1. Update debian anda

#apt update

```
root@albi:~# apt update
Hit:1 http://deb.debian.org/debian bookworm InRelease
Get:2 http://deb.debian.org/debian bookworm-updates InRelease [55,4 kB]
Hit:3 http://security.debian.org/debian-security bookworm-security InRelease
Fetched 55,4 kB in 6s (9.330 B/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
79 packages can be upgraded. Run 'apt list --upgradable' to see them.
root@albi:~#
```

Activate W
Go to Settings

2. Install Squid

#apt install squid

```
root@albi:~# apt install squid
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libdbi-perl libecap3 squid-common squid-langpack
Suggested packages:
  libmldbm-perl libnet-daemon-perl libsql-statement-perl squidclient squid-cgi squid-purge resolvconf
  ufw winbind
The following NEW packages will be installed:
  libdbi-perl libecap3 squid squid-common squid-langpack
0 upgraded, 5 newly installed, 0 to remove and 79 not upgraded.
Need to get 4.166 kB of archives.
After this operation, 16,7 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://security.debian.org/debian-security bookworm-security/main amd64 squid-common all 5.7-2+deb
```

3. Backup dulu file /etc/squid/squid.conf

#cp /etc/squid/squid.conf /etc/squid/squid.conf.orig

```
root@albi:~# cp /etc/squid/squid.conf /etc/squid/squid.conf.orig
root@albi:~#
```

4. Buka dan edit file konfigurasi squid.

Jika anda menggunakan nano, anda dapat menggunakan ctrl w untuk

mencari baris berikut :

INSERT YOUR OWN RULE(S)

Setting http_access

- Dibawah baris INSERT YOUR .., carilah

http_access allow localhost.

- Pastikan bahwa tertulis

http_access allow localhost

- Dibawah baris tersebut, carilah

http_access deny all.

- Berikan tanda # di depan http_access

deny all, untuk menonaktifkan

konfigurasi tersebut

- Tambahkan: http_access allow all

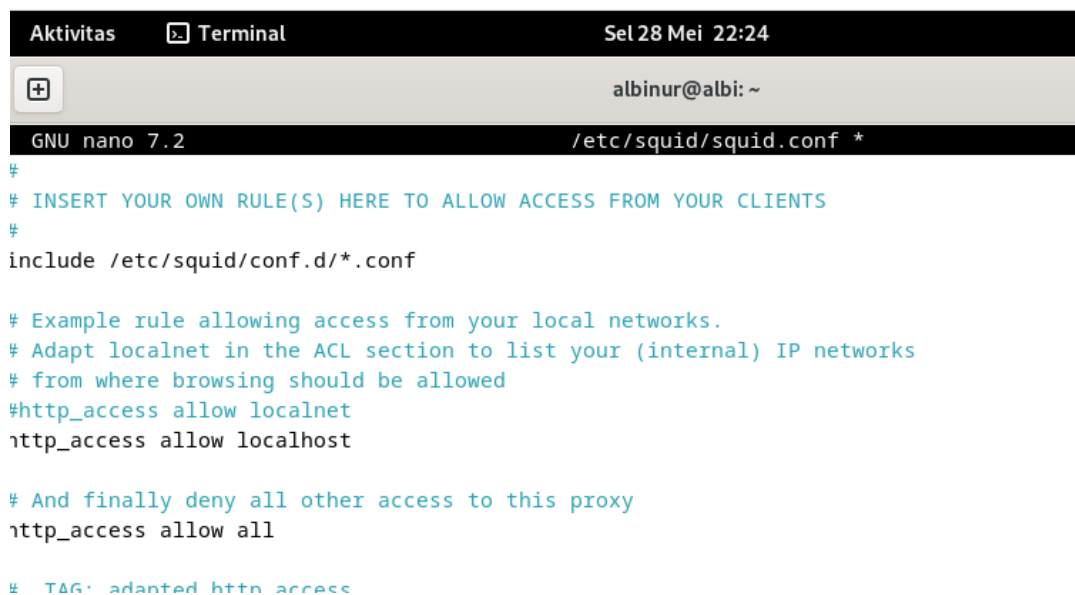
- Ketikkan baris berikut dibawahnya

http_access allow all

- Tujuannya agar semua Client dapat

mengakses protocol http via Proxy

Server tersebut.



```
Aktivitas  Terminal  Sel 28 Mei 22:24
albinur@albi: ~
GNU nano 7.2  /etc/squid/squid.conf *
#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#
include /etc/squid/conf.d/*.conf

# Example rule allowing access from your local networks.
# Adapt localnet in the ACL section to list your (internal) IP networks
# from where browsing should be allowed
#http_access allow localnet
http_access allow localhost

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

# TAG: adapted http access
```

Setting http_port

- Setelah setting http_access, sekarang lakukan setting konfigurasi port
- Secara default, proxy server menggunakan port 3128
- Selain 3128, proxy server banyak menggunakan port 80,443,8080
- Namun, anda dapat mengubah sesuai keinginan anda, asalkan jangan menggunakan port yang dipakai oleh server lain.
- Misal : dns menggunakan port 53, smtp menggunakan port 25, dll
- Jika anda punya webserver pada PC yang sama, jangan gunakan port 80 untuk proxy

- Carilah baris http_port dan tuliskan port yang dipakai

http_port 3128

- Save dan Exit



```
Aktivitas Terminal Sel 28 Mei 22:27
albinur@albi: ~
GNU nano 7.2 /etc/squid/squid.conf *
#
# Squid normally listens to port 3128
http_port 3128
# TAG: https_port
# Usage: [ip:]port [mode] tls-cert=certificate.pem [options]
#
```

2. Server : Cek IP address server

5. Cek ip address squid server.

```
root@albi:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:ac:95:ce brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.1.70/24 brd 192.168.1.255 scope global dynamic noprefixroute ens33
        valid_lft 81829sec preferred_lft 81829sec
    inet6 fe80::20c:29ff:feac:95ce/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

3. Server: Restart Squid

- Setiap ada perubahan squid.conf, restart squid untuk mengaktifkan perubahan konfigurasi
- Cek statusnya, pastikan Active: active (running)

```
root@albi:~# systemctl restart squid
```

```
^C
```

```
root@albi:~# systemctl status squid
```

```
● squid.service - Squid Web Proxy Server
   Loaded: loaded (/lib/systemd/system/squid.service; enabled; preset: enabled)
   Active: active (running) since Tue 2024-05-28 22:44:41 WIB; 4s ago
     Docs: man:squid(8)
  Process: 5542 ExecStartPre=/usr/sbin/squid --foreground -z (code=exited, status=0/SUCCESS)
 Main PID: 5545 (squid)
    Tasks: 4 (limit: 2252)
   Memory: 16.1M
      CPU: 283ms
   CGroup: /system.slice/squid.service
           └─5545 /usr/sbin/squid --foreground -sYC
             └─5547 "(squid-1)" --kid squid-1 --foreground -sYC
               └─5548 "(logfile-daemon)" /var/log/squid/access.log
                 └─5549 "(pinger)"
```

```
Mei 28 22:44:41 albi squid[5547]: Using Least Load store dir selection
```

```
Mei 28 22:44:41 albi squid[5547]: Set Current Directory to /var/spool/squid
```

```
Mei 28 22:44:41 albi squid[5547]: Finished loading MIME types and icons.
```

```
Mei 28 22:44:41 albi squid[5547]: HTCP Disabled.
```

```
Mei 28 22:44:41 albi squid[5547]: Pinger socket opened on FD 14
```

```
Mei 28 22:44:41 albi squid[5547]: Squid plugin modules loaded: 0
```

```
Mei 28 22:44:41 albi squid[5547]: Adaptation support is off.
```

```
Mei 28 22:44:41 albi squid[5547]: Accepting HTTP Socket connections at conn3 local=[::]:3128 remote=[::]:>
```

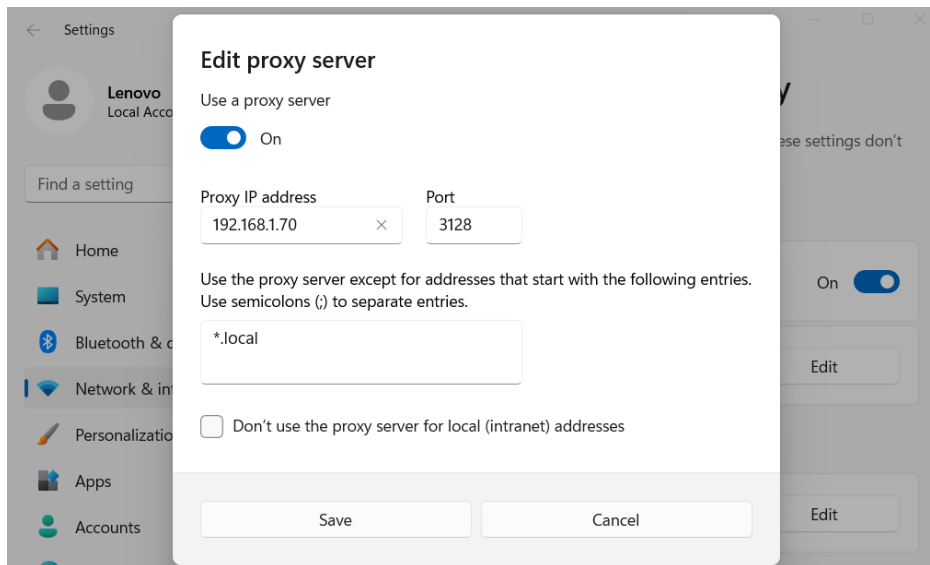
```
Mei 28 22:44:41 albi systemd[1]: Started squid.service - Squid Web Proxy Server
```

```
Mei 28 22:44:42 albi squid[5547]: storeLateRelease: released 0 objects
```

```
lines 1-25/25 (END)
```

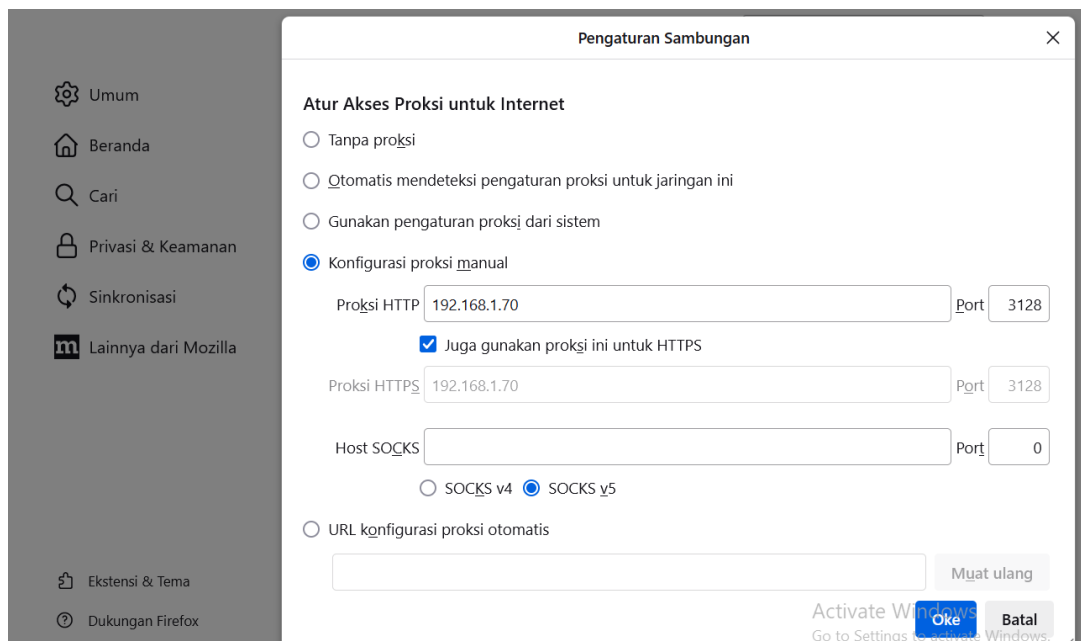
4. Client : Setting proxy – Chrome

- Buka Chrome
- Klik tanda
- Klik Settings, dibagian bawah menu
- Ketikkan proxy di window search atas
- Pada bagian Manual proxy setup, klik Set up
- Masukkan nomor IP dan port proxyserver di Address dan Port.
- Samakan dengan nomor IP Server
- Klik Save



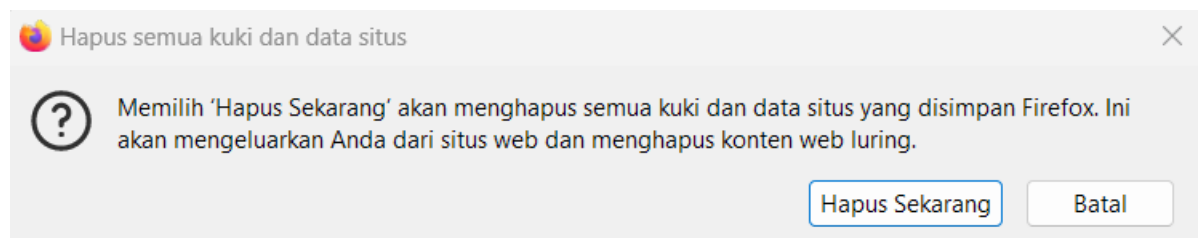
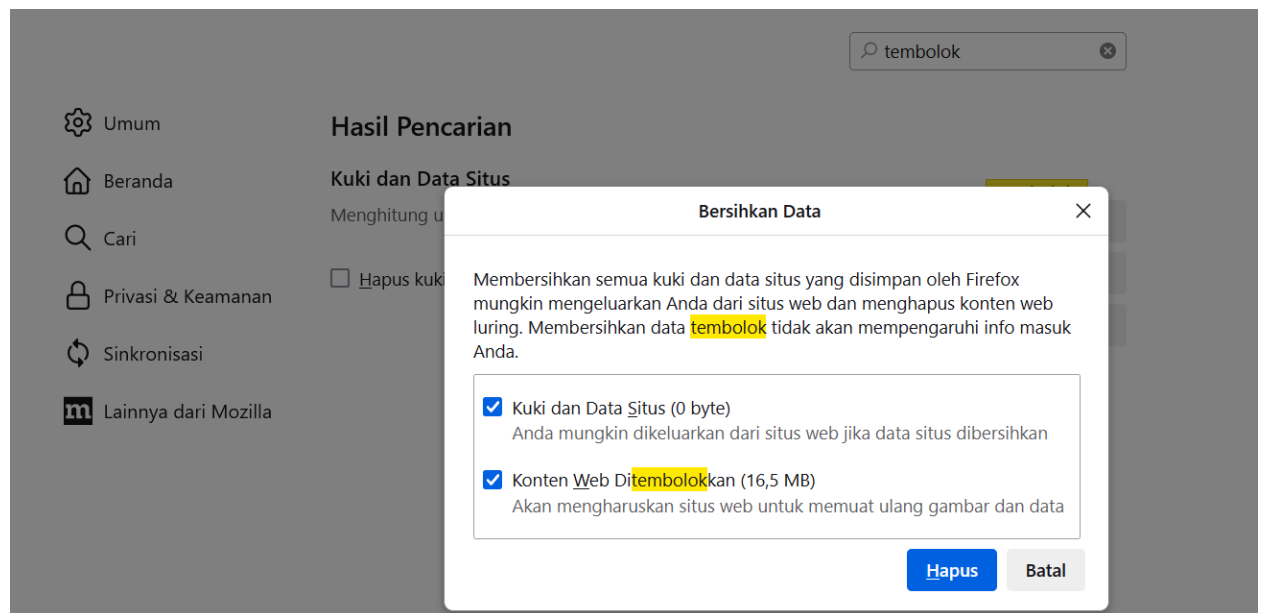
4. Client : Setting proxy di - Firefox

- Klik tanda di pojok kanan atas
- Klik Settings di bagian bawah
- Ketikkan proxy pada window search
- Pada Network Settings, klik Settings...
- Klik : Manual Proxy Configuration.
- Masukkan IP dan Port proxy server
- Klik OK



5. Client: Bersihkan cache browser (Firefox)

- Klik di pojok kanan atas
- Klik Settings
- Pada window search, ketikkan cache
- Pada Search Results, klik Clear Data
- Pada Clear Data, klik Cookies and Site Data dan Cached Web Content
- Klik Clear
- Pada Clear all cookies and site data, klik Clear Now
- Buka lagi Clear Data, pastikan Cookies and Site Data dan Cached Web Content bernilai 0 bytes



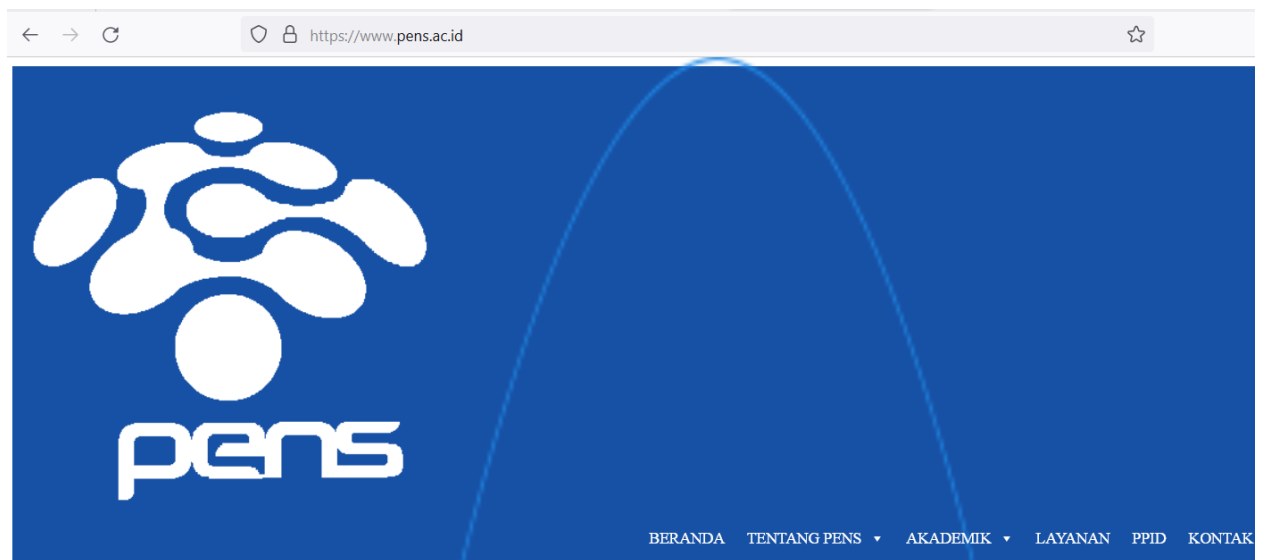
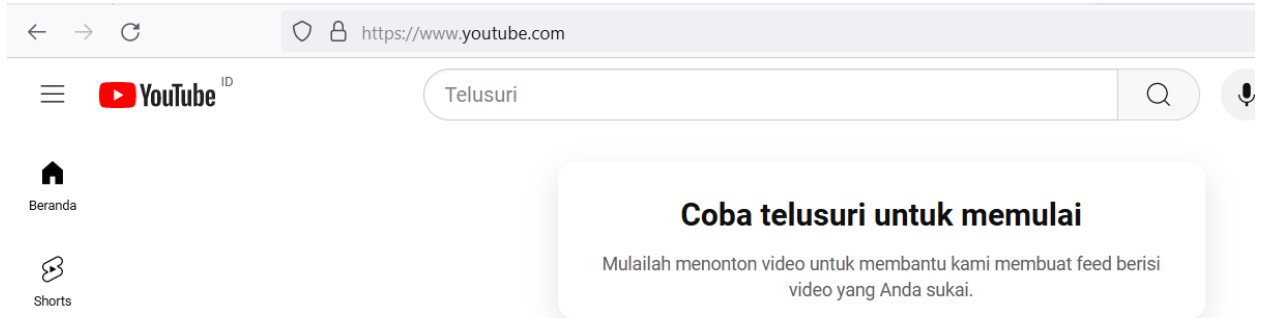
Hasil Pencarian

Kuki dan Data Situs

Kuki, data situs tersimpan, dan tembolok Anda saat ini menggunakan ruang penyimpanan 0 byte. [Pelajari lebih lanjut](#)

6. Client : Testing Proxy Server

- Buka browser dan coba cek apakah www.youtube.com dan www.pens.ac.id bisa diakses
- Hasil: Kedua domain dapat dibuka dengan baik



7. Server : Testing Proxy Server

- Ada banyak cara untuk mengetes server.
- Kita dapat menggunakan perintah ss, ps, ataupun melihat file access.log dan cache.log

SS

- Ss adalah singkatan dari socket statistics, perintah ini digunakan untuk mengecek semua koneksi socket

- Opsi :

-n : menampilkan secara ip numerik, bukan dalam bentuk nama domain
-l : menampilkan semua socket yang dalam keadaan listening
-a : menampilkan semua socket yang dalam keadaan listening atau tidak
-t : menampilkan semua socket dengan protocol tcp
-u : menampilkan semua socket dengan protocol udp
-p : menampilkan pid proses

Output ss

```
$ ss -t
```

```
State Recv-Q Send-Q Local Address:Port Peer Address:Port
```

```
ESTAB 0 0 192.168.43.4:38658 142.250.183.2:https
```

- Dimana :

<socket-type> <status> <recv-Q> <send-Q> <src_addr: port> <dest_addr,port>

<socket-type> : Bisa berupa TCP, UDP, SOCK_SEQPACKET, dan ICMP

<status> - Status socket. Bisa berupa SYN-RECV, SYN-SENT, TIME-WAIT, atau ESTB (established).

<recv-Q> - Jumlah paket yang diterima queue

<send-Q> - Jumlah paket yang kirim dari queue.

<src_addr: port> - Alamat IP source dan port source

<dest_address:port>- Alamat IP tujuan dan port tujuan

Pengetesan dengan ss

- Output:

Ss menunjukkan bahwa squid menggunakan tcp, status listening pada

port 3128, pid 6868

0.0.0.0, menunjukkan bahwa ip bersikap local, karena digunakan vmware

```
root@albi:~# ss -nlptu | grep squid
udp    UNCONN 0      0      0.0.0.0:36039    0.0.0.0:*    users:({ "squid",pid=5547,fd=9})

udp    UNCONN 0      0      *:43156         *:          users:({ "squid",pid=5547,fd=8})

tcp    LISTEN 0      256     *:3128         *:          users:({ "squid",pid=5547,fd=12})

root@albi:~#
```

Pengetesan dengan ps

- Untuk melihat pid server, gunakan perintah ps, ada beberapa proses

yang dibangkitkan oleh squid,

```
root@albi:~# ps aux | grep squid
root      5545  0.0  0.9 66372 19532 ?        Ss   22:44   0:00 /usr/sbin/squid --foreground -sYC
proxy     5547  0.9  1.5 77912 31204 ?        S    22:44   0:23 (squid-1) --kid squid-1 --foreground
proxy     5548  0.0  0.0  5644  1872 ?        S    22:44   0:00 (logfile-daemon) /var/log/squid/access
s.log
root      5706  0.0  0.1  6540  2228 pts/0    S+   23:26   0:00 grep squid

root@albi:~#
```

Mengecek isi access.log

- Melihat isi access.log dengan cat, kemudian difilter dengan grep

- Pada baris pertama, client (192.168.45.72) mencoba mengakses

youtube dengan perintah get

- Pada baris pertama, client (192.168.45.72) telah terkoneksi dengan

youtube dari status CONNECT

```
root@albi:~# cat /var/log/squid/access.log | grep www.youtube.com
1716912157.489 29708 192.168.1.40 TCP_TUNNEL/200 306737 CONNECT www.youtube.com:443 - HIER_DIRECT/142.251.12.93 -
1716912167.492 7248 192.168.1.40 TCP_TUNNEL/200 2874 CONNECT www.youtube.com:443 - HIER_DIRECT/142.251.12.93 -
1716912207.549 9234 192.168.1.40 TCP_TUNNEL/200 7383 CONNECT www.youtube.com:443 - HIER_DIRECT/142.251.10.136 -
1716912217.575 2169 192.168.1.40 TCP_TUNNEL/200 3350 CONNECT www.youtube.com:443 - HIER_DIRECT/142.251
```

- Nampak, client berhasil terkoneksi dengan youtube

- Sekarang di client, buka browser <http://www.pens.ac.id>

- Lihat isi access.log

```
root@albi:~# cat /var/log/squid/access.log | grep www.pens.ac.id
1716912538.919 2032 192.168.1.40 TCP_TUNNEL/200 225604 CONNECT www.pens.ac.id:443 - HIER_DIRECT/202.9.85.176 -
1716912539.376 2480 192.168.1.40 TCP_TUNNEL/200 151681 CONNECT www.pens.ac.id:443 - HIER_DIRECT/202.9.85.176 -
1716912539.383 3661 192.168.1.40 TCP_TUNNEL/200 276832 CONNECT www.pens.ac.id:443 - HIER_DIRECT/202.9.85.176 -
1716912539.387 2493 192.168.1.40 TCP_TUNNEL/200 149901 CONNECT www.pens.ac.id:443 - HIER_DIRECT/202.9.85.176 -
```

- Jika anda gagal melihat apapun di access.log untuk youtube atau www.pens.ac.id,

kemungkinan disebabkan squid tidak bisa melogging ketika yang diakses adalah situs https.

- Squid hanya bisa melogging situs http.

- Untuk mencoba situs http, anda bisa mencoba lecturer.pens.ac.id

- Buka browser <http://lecturer.pens.ac.id>
- Di Server, cek isi log : `grep .pens.ac.id` akan memfilter semua kata yang mengandung

`pens.ac.id`

```
root@albi:~# cat /var/log/squid/access.log | grep .pens.ac.id
1716912538.919 2032 192.168.1.40 TCP_TUNNEL/200 225604 CONNECT www.pens.ac.id:443 - HIER_DIRECT/202.9.85.176 -
1716912539.376 2480 192.168.1.40 TCP_TUNNEL/200 151681 CONNECT www.pens.ac.id:443 - HIER_DIRECT/202.9.85.176 -
1716912539.383 3661 192.168.1.40 TCP_TUNNEL/200 276832 CONNECT www.pens.ac.id:443 - HIER_DIRECT/202.9.85.176 -
1716912539.387 2493 192.168.1.40 TCP_TUNNEL/200 149901 CONNECT www.pens.ac.id:443 - HIER_DIRECT/202.9.85.176 -
```

Mengecek isi `cache.log`

- File `/var/log/squid/cache.log` melogging semua informasi yang terjadi pada proxy server
- `cache.log` menyimpan info mulai dari awal proxy dijalankan s/d saat terakhir

proxy bekerja

- Saat squid direstart, informasi ini juga akan di log di file ini
- Melihat seluruh isi `cache.log`

`#cat /var/log/squid/cache.log`

- Melihat hanya perubahan terakhir dari `cache.log`

`#tail -f /var/log/squid/cache.log`

- Sering kali hasil cek di

```
root@albi:~# cat /var/log/squid/cache.log
cat: /var/log/squid/cache.log: Tidak ada berkas atau direktori seperti itu
root@albi:~# cat /var/log/squid/cache.log
2024/05/28 22:16:50 kid1| Set Current Directory to /var/spool/squid
2024/05/28 22:16:50 kid1| Creating missing swap directories
2024/05/28 22:16:50 kid1| No cache_dir stores are configured.
2024/05/28 22:16:50 kid1| Removing PID file (/run/squid.pid)
2024/05/28 22:16:50 kid1| Set Current Directory to /var/spool/squid
2024/05/28 22:16:50 kid1| Starting Squid Cache version 5.7 for x86_64-pc-linux-gnu...
2024/05/28 22:16:50 kid1| Service Name: squid
2024/05/28 22:16:50 kid1| Process ID 5394
2024/05/28 22:16:50 kid1| Process Roles: worker
2024/05/28 22:16:50 kid1| With 1024 file descriptors available
2024/05/28 22:16:50 kid1| Initializing IP Cache...
2024/05/28 22:16:50 kid1| DNS Socket created at [::], FD 8
2024/05/28 22:16:50 kid1| DNS Socket created at 0.0.0.0, FD 9
2024/05/28 22:16:50 kid1| Adding nameserver 192.168.1.1 from /etc/resolv.conf
2024/05/28 22:16:50 kid1| Adding nameserver fe80::1%ens33 from /etc/resolv.conf
2024/05/28 22:16:50 kid1| Logfile: opening log daemon:/var/log/squid/access.log
2024/05/28 22:16:50 kid1| Logfile Daemon: opening log /var/log/squid/access.log
2024/05/28 22:16:50 kid1| Local cache digest enabled; rebuild/rewrite every 3600/3600
2024/05/28 22:16:50 kid1| Store logging disabled
```

```
root@albi:~# tail -f /var/log/squid/cache.log
2024/05/28 23:30:06 kid1| NETDB state saved; 57 entries, 9 msec
2024/05/28 23:35:37| SendEcho ERROR: sending to ICMPv6 packet to [64:ff9b::4a7d:448a]: (101) Network is
unreachable
2024/05/28 23:46:53| SendEcho ERROR: sending to ICMPv6 packet to [2620:1ec:12::239]: (101) Network is u
reachable
2024/05/28 23:47:39| SendEcho ERROR: sending to ICMPv6 packet to [2600:9000:25fa:d800:3:a730:1900:93a1]
(101) Network is unreachable
2024/05/28 23:48:18| SendEcho ERROR: sending to ICMPv6 packet to [2603:1046:1400::7]: (101) Network is
nreachable
2024/05/28 23:50:05| SendEcho ERROR: sending to ICMPv6 packet to [2600:1901:1:c36::]: (101) Network is
nreachable
2024/05/28 23:50:27| SendEcho ERROR: sending to ICMPv6 packet to [64:ff9b::14cd:7366]: (101) Network is
```

2. Squid Proxy Server

1. Server : Bloking youtube

- Kita akan mengeblok youtube lewat squid
- Buka file `/etc/squid/squid.conf`
- Cari baris INSERT YOUR OWN RULE(S) dengan ctrl w.
- Tambahkan baris dibawah untuk bloking www.youtube.com

```
Aktivitas Terminal Rab 29 Mei 00:29
albinur@albi: ~
GNU nano 7.2 /etc/squid/squid.conf *

#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#
include /etc/squid/conf.d/*.conf

# Example rule allowing access from your local networks.
# Adapt localnet in the ACL section to list your (internal) IP networks
# from where browsing should be allowed
#http_access allow localnet
http_access allow localhost

acl blok_domain dstdomain www.youtube.com

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

# TAG: adapted_http_access
# Allowing or Denying access based on defined access lists
```

2. Server : Restart Squid

- Setiap ada perubahan di squid.conf, restart Squid. Perhatikan setiap kali kita melakukan restart squid, pidnya akan berubah

`#systemctl restart squid`

`#systemctl status squid`

```
root@albi:~# systemctl status squid
● squid.service - Squid Web Proxy Server
   Loaded: loaded (/lib/systemd/system/squid.service; enabled; preset: enabled)
   Active: active (running) since Wed 2024-05-29 00:33:17 WIB; 4s ago
     Docs: man:squid(8)
  Process: 6100 ExecStartPre=/usr/sbin/squid --foreground -z (code=exited, status=0/SUCCESS)
    Main PID: 6103 (squid)
      Tasks: 4 (limit: 2252)
     Memory: 16.6M
        CPU: 387ms
   CGroup: /system.slice/squid.service
           └─6103 /usr/sbin/squid --foreground -sYC
             └─6105 "(squid-1)" --kid squid-1 --foreground -sYC
               └─6106 "(logfile-daemon)" /var/log/squid/access.log
                 └─6107 "(pinger)"

Mei 29 00:33:17 albi squid[6105]: Using Least Load store dir selection
Mei 29 00:33:17 albi squid[6105]: Set Current Directory to /var/spool/squid
Mei 29 00:33:17 albi squid[6105]: Finished loading MIME types and icons.
Mei 29 00:33:17 albi squid[6105]: HTTP Disabled.
Mei 29 00:33:17 albi squid[6105]: Pinger socket opened on FD 14
Mei 29 00:33:17 albi squid[6105]: Squid plugin modules loaded: 0
Mei 29 00:33:17 albi squid[6105]: Adaptation support is off.
Mei 29 00:33:17 albi squid[6105]: Accepting HTTP Socket connections at conn3 local=[::]:3128 remote=[::]:
Mei 29 00:33:17 albi systemd[1]: Started squid.service - Squid Web Proxy Server.
Mei 29 00:33:18 albi squid[6105]: storeLateRelease: released 0 objects
lines 1-25/25 (END)
```

3. Server : Cek IP Address Server

- Cek nomor IP server.
- Ternyata nomor IP Proxy server berbeda dengan sebelumnya.
- Seharusnya server (semua jenis server) disetting IP addressnya secara statik, bukan secara dinamis dengan DHCP Server

```
root@albi:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:ac:95:ce brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.1.70/24 brd 192.168.1.255 scope global dynamic noprefixroute ens33
        valid_lft 74964sec preferred_lft 74964sec
    inet6 fe80::20c:29ff:feac:95ce/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
root@albi:~#
```

4. Client: Setting Proxy di Browser

- Masukkan nomor IP Server di browser
- Klik OK

Pengaturan Sambungan

Atur Akses Proksi untuk Internet

☐ Tanpa proksi

☐ Otomatis mendeteksi pengaturan proksi untuk jaringan ini

☐ Gunakan pengaturan proksi dari sistem

☒ Konfigurasi proksi manual

Proksi HTTP Port

☒ Juga gunakan proksi ini untuk HTTPS

Proksi HTTPS Port

Host SOCKS Port

☐ SOCKS v4 ☒ SOCKS v5

☐ URL konfigurasi proksi otomatis

Muat ulang

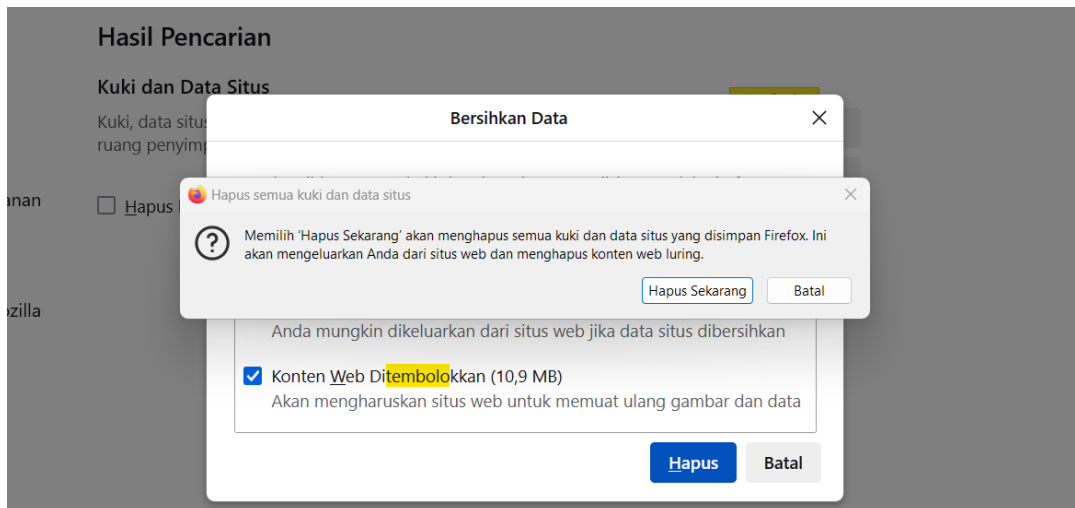
Oke Batal

5. Client: Bersihkan cache browser (Firefox)

- Klik di pojok kanan atas
- Klik Settings
- Pada window search, ketikkan cache
- Pada Search Results, klik Clear Data
- Pada Clear Data, klik Cookies and Site Data

dan Cached Web Content

- Klik Clear
- Pada Clear all cookies and site data, klik Clear Now
- Buka lagi Clear Data, pastikan Cookies and Site Data dan Cached Web Content bernilai 0 bytes



Hasil Pencarian

Kuki dan Data Situs

Kuki, data situs tersimpan, dan tembolok Anda saat ini menggunakan ruang penyimpanan 0 byte. [Pelajari lebih lanjut](#)

☐ Hapus kuki dan data situs ketika Firefox ditutup

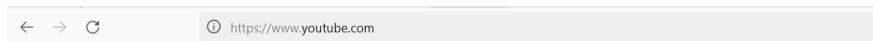
6.Client : Test Bloking Youtube

- Buka halaman web berikut

www.youtube.com, www.pens.ac.id,

www.facebook.com

- Proxy server sukses mengeblok youtube.
- Proxy server tetap bisa mengakses facebook dan pens.ac.id

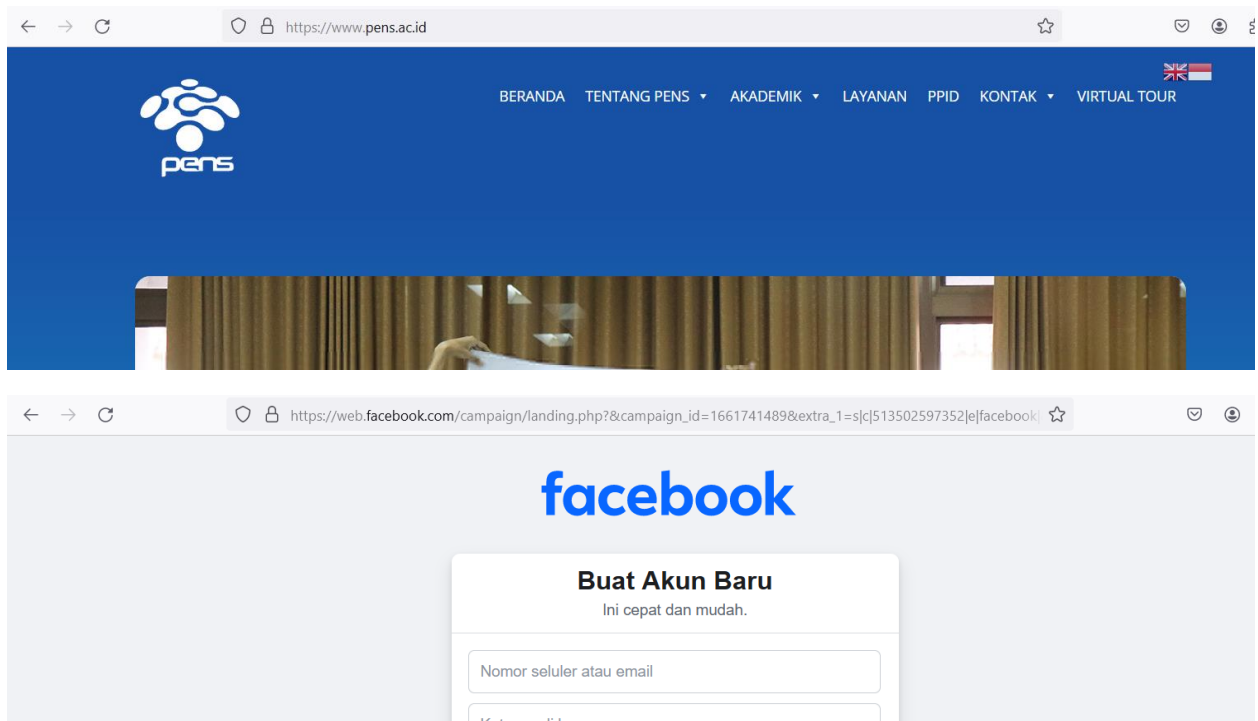


Server proksi menolak sambungan

Terjadi kesalahan ketika menyambungkan ke www.youtube.com.

- Periksa pengaturan proksi, pastikan sudah benar.
- Hubungi administrator jaringan Anda untuk memastikan server proksi sudah berjalan.

Coba Lagi



7. Server : Bloking subdomain pens.ac.id

- Pens memiliki beberapa subdomain seperti lecturer.pens.ac.id, webmail.pens.ac.id, www.pens.ac.id, dll. Kita akan mengeblok semua subdomain tersebut
- Domain youtube tetap diblok
- Domain lainnya di-allow

1. Tambahkan baris berikut di squid.conf

```
acl blok_domain dstdomain www.youtube.com
```

```
acl blok_domain dstdomain .pens.ac.id
```

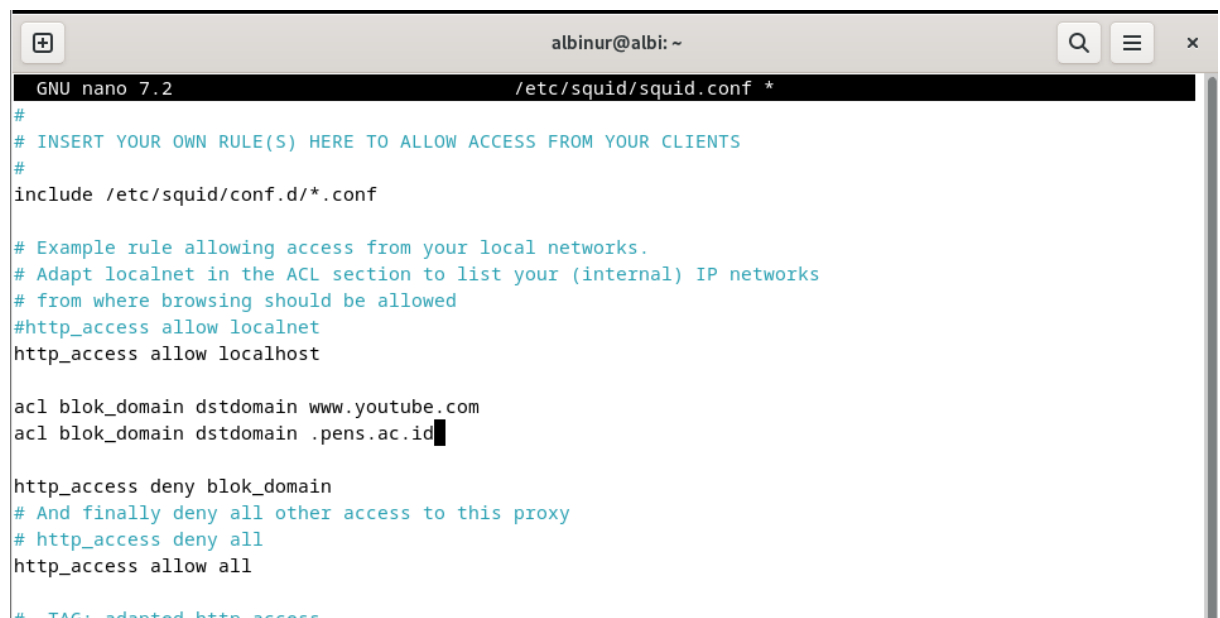
```
http_access deny blok_domain
```

```
http_access allow all
```

Save dan exit

2. Restart squid dan cek statusnya

3. Cek IP server

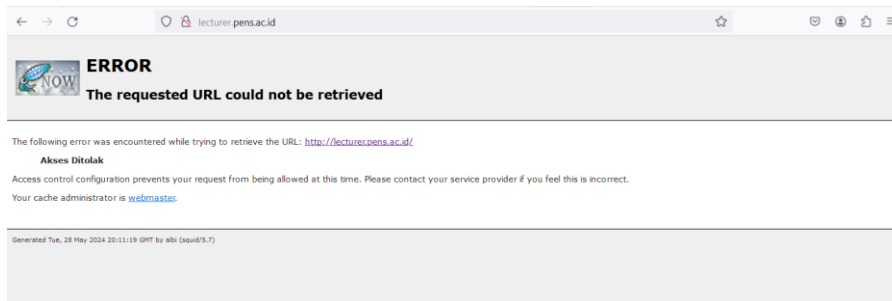


```
albinur@albi: ~  
GNU nano 7.2 /etc/squid/squid.conf *  
#  
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS  
#  
include /etc/squid/conf.d/*.conf  
  
# Example rule allowing access from your local networks.  
# Adapt localnet in the ACL section to list your (internal) IP networks  
# from where browsing should be allowed  
#http_access allow localnet  
http_access allow localhost  
  
acl blok_domain dstdomain www.youtube.com  
acl blok_domain dstdomain .pens.ac.id  
  
http_access deny blok_domain  
# And finally deny all other access to this proxy  
# http_access deny all  
http_access allow all  
# TAG: adapted http access
```

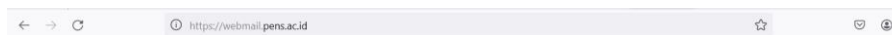
8. Client : Bloking subdomain pens.ac.id

1. Pastikan setting proxy di browser client telah menggunakan nomor IP server yang benar
2. Bersihkan cache browser client, pastikan sudah 0 bytes
3. Buka browser di client. Ketikkan lecturer.pens.ac.id, webmail.pens.ac.id, www.pens.ac.id
4. Bisakah ketiga subdomain tersebut dibuka ?

lecturer.pens.ac.id tidak bisa dibuka



Webmail.pens.ac.id tidak bisa dibuka



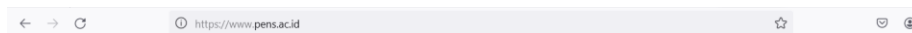
Server proksi menolak sambungan

Terjadi kesalahan ketika menyambungkan ke webmail.pens.ac.id.

- Periksa pengaturan proksi, pastikan sudah benar.
- Hubungi administrator jaringan Anda untuk memastikan server proksi sudah berjalan.

Coba Lagi

www.pens.ac.id tidak bisa dibuka



Server proksi menolak sambungan

Terjadi kesalahan ketika menyambungkan ke www.pens.ac.id.

- Periksa pengaturan proksi, pastikan sudah benar.
- Hubungi administrator jaringan Anda untuk memastikan server proksi sudah berjalan.

Coba Lagi

9: Server: Allow satu subdomain, dan mengeblok subdomain lainnya

- Kita akan meng-allow webmail.pens.ac.id, namun mengeblok subdomain lainnya
- Domain youtube tetap diblok
- Domain lainnya di-allow

1. Tambahkan baris berikut di squid.conf

```
acl allow_domain dstdomain webmail.pens.ac.id
```

```
acl blok_domain dstdomain www.youtube.com
```

```
acl blok_domain dstdomain .pens.ac.id
```

```
http_access allow allow_domain
```

```
http_access deny blok_domain
```

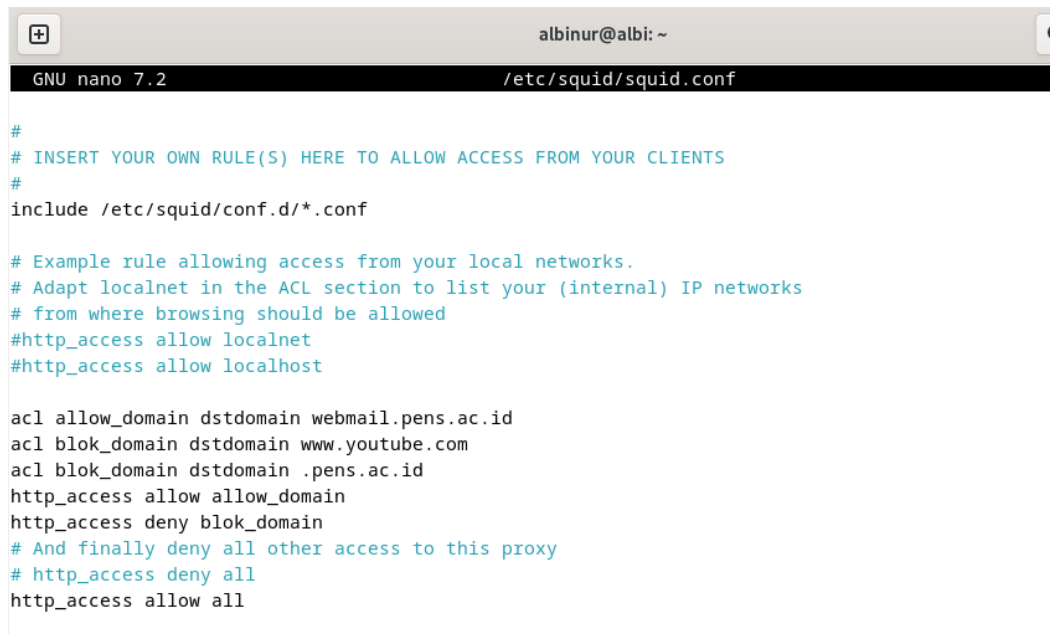
```
http_access allow all
```

Save dan exit

2. Restart squid dan cek statusnya

3. Cek IP server Perhatikan penulisan http_access allow untuk webmail sebelum http_access deny untuk semua subdomain.

http_access allow all akan melewatkan semua kecuali yang di deny



```
GNU nano 7.2 /etc/squid/squid.conf

#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#
include /etc/squid/conf.d/*.conf

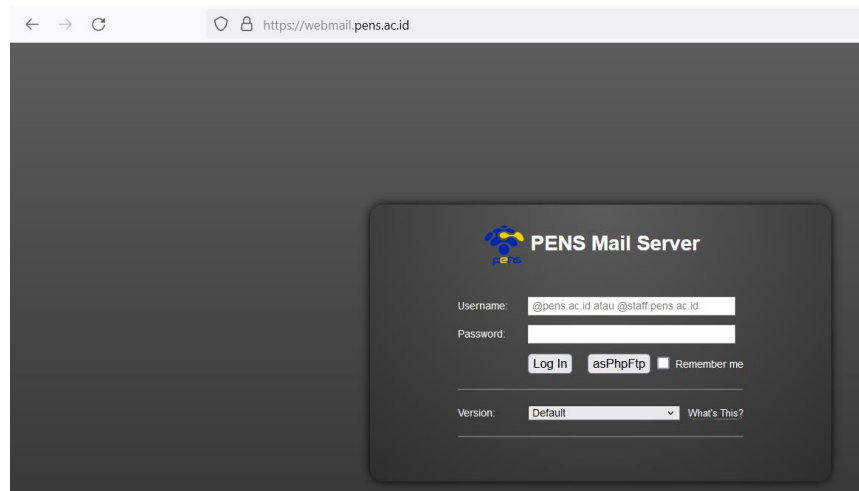
# Example rule allowing access from your local networks.
# Adapt localnet in the ACL section to list your (internal) IP networks
# from where browsing should be allowed
#http_access allow localnet
#http_access allow localhost

acl allow_domain dstdomain webmail.pens.ac.id
acl blok_domain dstdomain www.youtube.com
acl blok_domain dstdomain .pens.ac.id
http_access allow allow_domain
http_access deny blok_domain
# And finally deny all other access to this proxy
# http_access deny all
http_access allow all
```

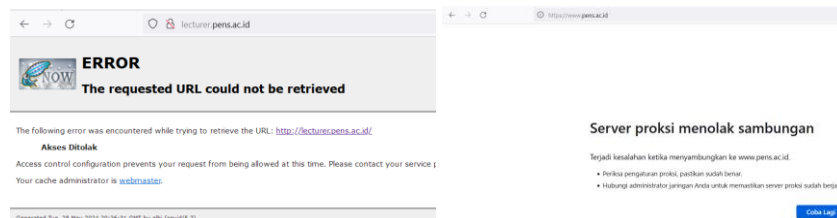
10. Client : Testing allow satu subdomain, dan mengeblok subdomain lainnya

1. Pastikan setting proxy di browser client telah menggunakan nomor IP server yang benar
2. Bersihkan cache browser client, pastikan sudah 0 bytes
3. Buka browser di client. Ketikkan lecturer.pens.ac.id, webmail.pens.ac.id, www.pens.ac.id
4. Bisakah ketiga subdomain tersebut dibuka ?

webmail.pens.ac.id bisa diakses



Sedangkan subdomain .pens.ac.id yang lain tetap tidak bisa



11. Server: Mengeblok IP Address Client

- Kita akan mengeblok IP address tertentu.
- Untuk itu kita akan menghapus blok ke youtube dan subdomain pens

1. Untuk memilih nomor IP yg hendak diblok, cek nomor IP address Client anda nomor IP address client dan catat. Disini digunakan 192.168.9.200

\$ip addr

2. Buka squid.conf

3. Tambahkan baris berikut di squid.conf

```
#acl allow_domain dstdomain webmail.pens.ac.id

# acl blok_domain dstdomain www.youtube.com

# acl blok_domain dstdomain .pens.ac.id

acl blok_pc src 192.168.9.200

# http_access allow allow_domain

# http_access deny blok_domain

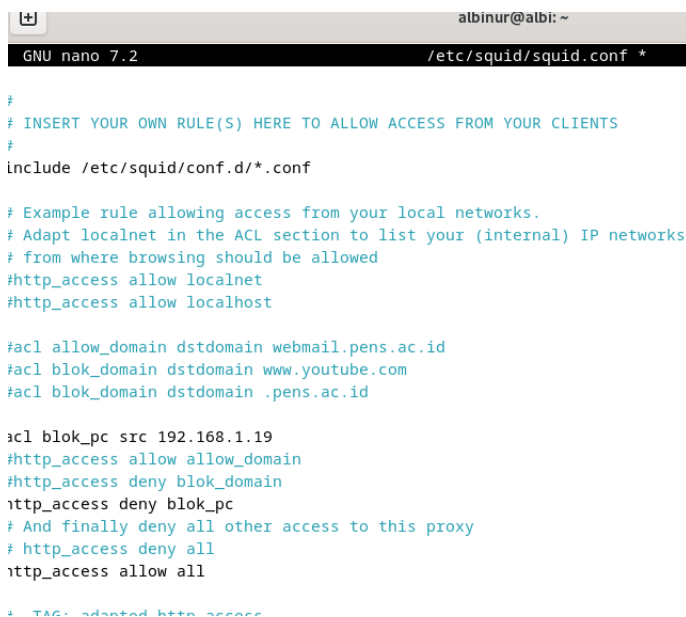
http_access deny blok_pc

http_access allow all
```

Save dan exit

4. Restart squid dan cek statusnya

5. Cek IP server



```
albinur@albi: ~
GNU nano 7.2 /etc/squid/squid.conf *

#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#
include /etc/squid/conf.d/*.conf

# Example rule allowing access from your local networks.
# Adapt localnet in the ACL section to list your (internal) IP networks
# from where browsing should be allowed
#http_access allow localnet
#http_access allow localhost

#acl allow_domain dstdomain webmail.pens.ac.id
#acl blok_domain dstdomain www.youtube.com
#acl blok_domain dstdomain .pens.ac.id

acl blok_pc src 192.168.1.19
#http_access allow allow_domain
#http_access deny blok_domain
http_access deny blok_pc
# And finally deny all other access to this proxy
# http_access deny all
http_access allow all

* TAG: adapted http access
```

12. Client : Testing blok IP client

1. Pastikan setting proxy di browser client telah menggunakan nomor IP server yang benar
2. Bersihkan cache browser client, pastikan sudah 0 bytes
3. Buka browser di client. Ketikkan www.youtube.com dan www.pens.ac.id
4. Bisakah 2 halaman web tersebut dibuka ?
5. Sekarang gantilah nomor ip address client.

Untuk mengganti nomor IP client, anda membutuhkan minimal 3 informasi, yaitu IP address, netmask dan gateway. Ganti IP address

dengan nomor IP yang masih satu network dengan Client.

Nomor IP client : 192.168.9.200/24. Nomor network: 192.168.9.0.

Nomor IP yang dapat dipakai: 192.168.9.1 sd 192.168.9.254. Pilihlah nomor IP yang belum dipakai dalam network anda. Misalkan server menggunakan 192.168.9.242, maka jangan gunakan nomor ini.

6. Cek gateway client

#ip route

Selain nomor ip server, nomor ip gateway jg tidak boleh dipakai. Cek dan catat. Misal nomor ip gateway 192.168.9.103.

7. Ubah nomor ip client.

- Misalkan dipilih nomor IP 192.168.9.250, netmask 255.255.255.0, gateway 192.168.9.103

- Buka `/etc/network/interfaces`

#nano `/etc/network/interfaces`

- Edit sebagai berikut :

Save dan exit.

- Restart service network & cek statusnya

`#systemctl restart networking`

`#systemctl status networking`

- Cek nomor ip yang baru

`#ip address`

- Ping ke gateway untuk memastikan ip baru telah bekerja

`#ping 192.168.9.250`

- Pastikan anda telah menggunakan nomor IP server yang benar di setting proxy di browser.
- Kosongkan cache browser client. Pastikan size cache 0
- Buka browser di client. Ketikkan www.youtube.com dan www.pens.ac.id
- Berhasilkah ?

Tidak berhasil

14. Client : Testing blok subnet/network address

1. Pastikan setting proxy di browser client telah menggunakan nomor IP server yang benar
2. Bersihkan cache browser client, pastikan sudah 0 bytes
3. Buka browser di client. Ketikkan www.youtube.com dan www.pens.ac.id
4. Bisakah 2 halaman web tersebut dibuka ?
5. Sekarang gantilah nomor ip address client. Gunakan nomor IP dalam satu subnet.

Untuk mengganti nomor IP client, anda membutuhkan minimal 3 informasi, yaitu IP address, netmask dan gateway. Ganti IP address dengan nomor IP yang masih satu network dengan Client.

Nomor IP client : 192.168.9.200/24. Nomor network: 192.168.9.0. Nomor IP yang dapat dipakai: 192.168.9.1 sd 192.168.9.254. Pilihlah nomor IP yang belum dipakai dalam network anda. Misalkan server menggunakan 192.168.9.242, maka jangan gunakan nomor ini.

6. Cek gateway client

```
#ip route
```

Selain nomor ip server, nomor ip gateway jg tidak boleh dipakai. Cek dan catat. Misal nomor ip gateway 192.168.9.103.

7. Ubah nomor ip client.

- Misalkan dipilih nomor IP 192.168.9.250, netmask 255.255.255.0, gateway 192.168.9.103
- Buka `/etc/network/interfaces`

```
#nano /etc/network/interfaces
```

- Edit sebagai berikut :

Save dan exit.

- Restart service network & cek statusnya

```
#systemctl restart networking
```

```
#systemctl status networking
```

- Cek nomor ip yang baru

```
#ip address
```

- Ping ke gateway untuk memastikan ip baru telah bekerja

```
#ping 192.168.9.250
```

- Pastikan anda telah menggunakan nomor IP server yang benar di setting proxy di browser.
- Kosongkan cache browser client. Pastikan size cache 0
- Buka browser di client. Ketikkan www.youtube.com dan www.pens.ac.id
- Berhasilkah ?

Tidak berhasil

3. Setting Autentikasi di Squid

Server : Setting password di Squid

- Cek apakah paket apache dan apache2-utils telah terinstall belum

```
root@albi:~# apt list apache2
Listing... Done
apache2/stable-security 2.4.59-1~deb12u1 amd64 [upgradable from: 2.4.57-2]
N: There is 1 additional version. Please use the '-a' switch to see it
root@albi:~# apt list apache2-utils
Listing... Done
apache2-utils/stable-security 2.4.59-1~deb12u1 amd64 [upgradable from: 2.4.57-2]
N: There is 1 additional version. Please use the '-a' switch to see it
```

- Jika sudah hapus dulu apache2 dan apache2-utils

```
root@albi:~# apt purge apache2
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  apache2-data apache2-utils
Use 'apt autoremove' to remove them.
The following packages will be REMOVED:
  apache2
0 upgraded, 0 newly installed, 1 to remove and 76 not upgraded.
After this operation, 508 kB disk space will be freed.
Do you want to continue? [Y/n] y
(Sedang membaca basis data ... 152185 berkas atau direktori telah terpasang.)
Removing apache2 (2.4.57-2) ...
Processing triggers for man-db (2.11.2-2) ...
(Sedang membaca basis data ... 152894 berkas atau direktori telah terpasang.)
Purging configuration files for apache2 (2.4.57-2) ...
dpkg: PERINGATAN: while removing apache2, directory '/var/www/html' not empty so not removed
dpkg: PERINGATAN: while removing apache2, directory '/etc/apache2/sites-available' not empty so not removed
root@albi:~# apt purge apache2-utils
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following package was automatically installed and is no longer required:
  apache2-data
Use 'apt autoremove' to remove it.
The following packages will be REMOVED:
  apache2-utils*
0 upgraded, 0 newly installed, 1 to remove and 77 not upgraded.
After this operation, 441 kB disk space will be freed.
Do you want to continue? [Y/n] y
(Sedang membaca basis data ... 151890 berkas atau direktori telah terpasang.)
Removing apache2-utils (2.4.57-2) ...
Processing triggers for man-db (2.11.2-2) ...
```

- Lakukan #apt autoremove

```
root@albi:~# apt autoremove
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages will be REMOVED:
  apache2-data
0 upgraded, 0 newly installed, 1 to remove and 76 not upgraded.
After this operation, 869 kB disk space will be freed.
Do you want to continue? [Y/n] y
(Sedang membaca basis data ... 151860 berkas atau direktori telah terpasang.)
Removing apache2-data (2.4.57-2) ...
```

- Buat 2 user : fitri dan yaya. Cek apa user tersebut sudah ada atau belum. Cek user fitri dan yaya di /etc/passwd

```
root@albi:~# cat /etc/passwd | grep fitri
fitri:x:1005:1005:,,,:/home/fitri:/bin/bash
root@albi:~# cat /etc/passwd | grep yaya
yaya:x:1006:1006:,,,:/home/yaya:/bin/bash
root@albi:~#
```

Sudah ada

- Install kembali apache2

#apt install apache2 apache2-utils

```
root@albi:~# apt install apache2 apache2-utils
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom
The following NEW packages will be installed:
  apache2 apache2-data apache2-utils
The following packages will be upgraded:
  apache2-bin
1 upgraded, 3 newly installed, 0 to remove and 75 not upgraded.
```

- Buat file password squid. Perhatikan bahwa password user di squid ini sebaiknya sama dengan password user yang dibuat di langkah 2. Jika tidak, maka user tidak akan bisa login.

```
#htpasswd -c /etc/squid/passwd yaya
```

```
#htpasswd -c /etc/squid/passwd fitri
```

```
root@albi:~# htpasswd -c /etc/squid/passwd yaya
New password:
Re-type new password:
Adding password for user yaya
root@albi:~# htpasswd -c /etc/squid/passwd fitri
New password:
Re-type new password:
Adding password for user fitri
```

Ac
Go

Server : Membangun otentikasi di Squid

- Buka file konfigurasi squid.conf
- Cari kata auth_param basic dengan Ctrl w
- Tambahkan text di bagian bawah tag auth_param

```
#Default:
# none
auth_param basic program /usr/lib/squid/basic_ncsa_auth /etc/squid/passwd
auth_param basic children 5
auth_param basic realm fitri123
auth_param basic realm yaya123
auth_param basic credentialsttl 5 hours
acl otentikasi proxy_auth REQUIRED
http_access allow otentikasi

# TAG: authenticate cache garbage interval
```

- Simpan dan Exit
- Restart squid

```
#systemctl restart squid
```

- Cek statusnya

```
#systemctl status squid
```

```
root@albi:~# systemctl restart squid
root@albi:~# systemctl status squid
● squid.service - Squid Web Proxy Server
   Loaded: loaded (/lib/systemd/system/squid.service; enabled; preset: enabled)
   Active: active (running) since Wed 2024-05-29 13:42:35 WIB; 11s ago
```

Tag <auth_param>

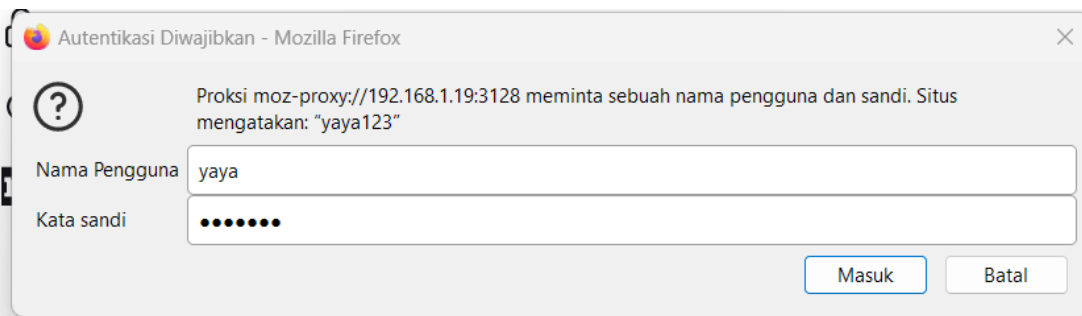
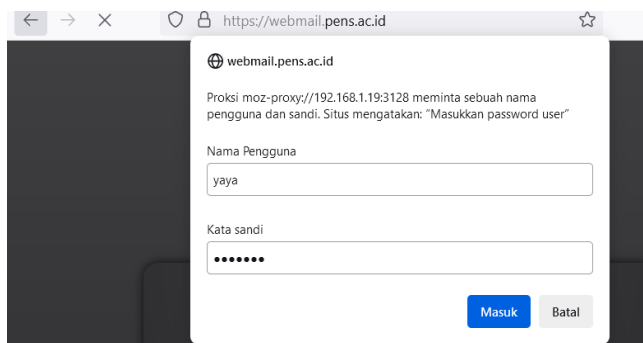
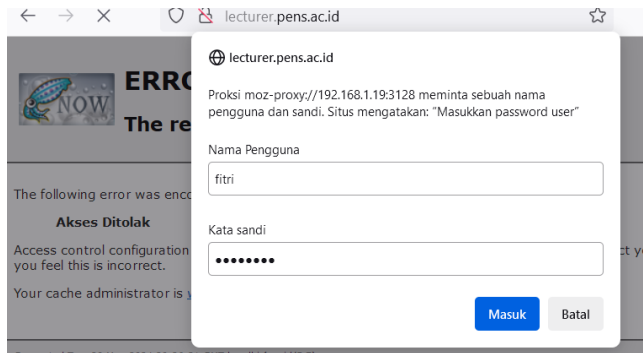
- auth_param basic program </usr/lib/squid/basic_ncsa_auth> </etc/squid/passwd>
- Modul executable otentikasi ada : di /usr/lib/squid/basic_ncsa_auth , sementara file password ada di : /etc/squid/passwd
- auth_param basic children <5>
 - Jumlah otentikasi maksimum yang dapat dilayani oleh squid
- auth_param basic realm <Masukkan password user>
 - String yang akan dilihat user saat otentikasi proxy. Nilai default adalah Squid proxy-caching web server
- auth_param basic credentialsttl 5 hours
 - Jangka waktu maksimum user dapat login di proxy server

ACL otentikasi

- acl otentikasi proxy_auth REQUIRED
- http_access allow otentikasi

Client :

- Buka browser client
- Masukkan username dan password



- Buka www.pens.ac.id, lecturer.pens.ac.id, it.pens.ac.id

4. SARG

SARG

1. Download Sarg dari <https://sourceforge.net/projects/sarg>

2. Pindah ke directory /opt/ dan dekompresi file tersebut

```
#mv /home/fitri/Downloads/sarg-2.4.0.tar.gz /opt/
```

```
#cd /opt
```

```
#tar xvfz sarg-2.4.0.tar.gz
```

```
#cd sarg-2.4.0
```

3. Install dulu semua dependensi dari Sarg

```
#apt install build-essential
```

```
#apt install zlib1g-dev libgd-dev libbz2-dev liblzma-dev libldap2-dev
```

```
#apt install libpcre3-dev
```

4. Pada directory /opt/sarg-2.4.0, lakukan configure

```
#cd /opt/sarg-2.4.0
```

```
#./configure
```

Jika tidak terjadi error, maka akan terbentuk Makefile seperti gambar

dibawah. Sepanjang semua file dependensi telah diinstall seperti

langkah 3), tidak akan terjadi error

5. Lakukan make

```
#cd /opt/sarg-2.4.0
```

```
#make
```

- Nampak output seperti berikut:

- Error pada file index.c

- Solusi :

- Pada file index.c,

cari baris `char yearnum[10];`

- Ubah menjadi `char yearnum[20];`

- Simpan dengan Ctrl O
- Lakukan make lagi

#make

- Nampak output seperti berikut:
- Error pada file userinfo.c
- Solusi :

- Pada file userinfo.c, cari baris char cstr[9]; dengan Ctr W.
- Ubah menjadi char cstr[90];
- Simpan dengan Ctrl O.
- Lakukan make lagi

#make

- Output make yang
- tanpa error. Semua file terkompilasi dengan baik

8. Setelah berhasil, lakukan make install

```
#mkdir /home/sarg-2.4.0
```

```
#make install DESTDIR=/home/sarg-2.4.0
```

Jika tak ada pesan error, berarti instalasi sukses

9. Sekarang, jalankan sarg. Binary sarg terletak di /home/sarg-2.4.0/usr/local/bin/

```
#cd /home/sarg-2.4.0/usr/local/bin/
```

```
#./sarg -x
```

- Ada error :

Sarg tidak dapat menemukan file tersebut

10. Copy kan file konfigurasi sarg ke /usr/local/etc/

```
#cp /home/sarg-2.4.0/usr/local/etc/sarg.conf /usr/local/etc/sarg.conf
```

11. Ulangi langkah 9

```
#cd /home/sarg-2.4.0/usr/local/bin/
```

```
#./sarg -x
```

Muncul error tentang file /usr/local/etc/exclude_codes

Sarg tidak dapat menemukan file tersebut

11. Copy kan file exclude_codes ke /usr/local/etc/

```
#cp /home/sarg-2.4.0/usr/local/etc/exclude_codes /usr/local/etc/
```

12. Ulangi langkah 9

```
#cd /home/sarg-2.4.0/usr/local/bin/
```

```
#./sarg -x
```

Muncul error

13. Copykan directory /home/sarg-2.4.0/usr/local/share ke /usr/local/share

```
#cp -r /home/sarg-2.4.0/usr/local/share/ /usr/local/share/
```

14. Ulangi langkah 9

```
#cd /home/sarg-2.4.0/usr/local/bin/
```

```
#./sarg -x
```

15. Di bagian bawah, tertulis report tergenerate di /var/www/html/squid-reports/

- Anda sukses mengenerate report sarg

16. Buka browser, ketikkan <http://www.fitri.edu/squid-reports> Keluar output berikut

17. Buka file /etc/apache2/sites-available/www.fitri.edu.conf dan edit

sbb :

18. Sekarang, reload dan restart apache2

```
#systemctl reload apache2
```

```
#systemctl restart apache2
```

19. Buka browser, ketikkan <http://www.fitri.edu/squid-reports>

Keluar output berikut:

- Klik salah satu link yang ditunjuk panah, maka akan muncul output berikut :