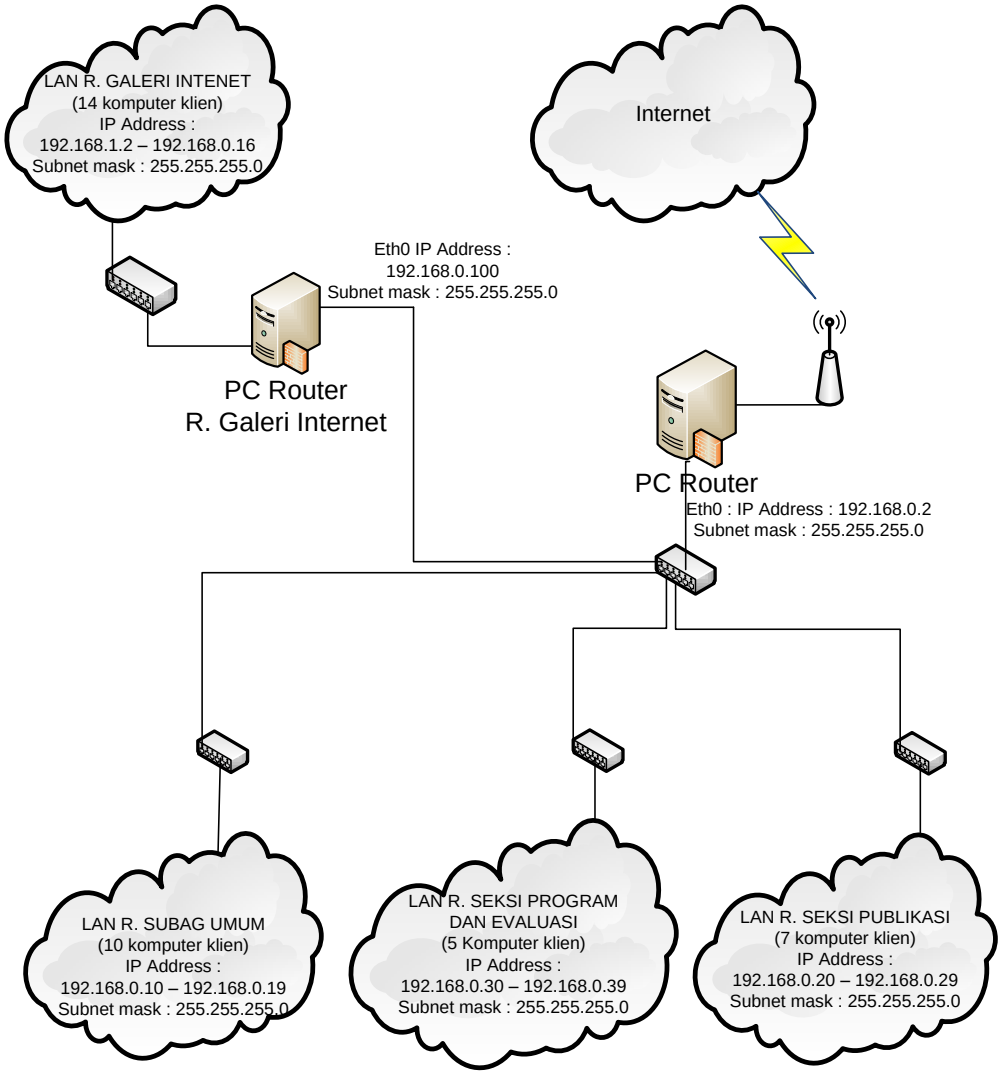
BAB III
PEMBAHASAN

3.1. Data Jaringan Komputer Eksisting BPPKI Bandung

Berikut ini adalah data jaringan komputer eksisting (*Local Area Network/LAN*) di kantor BPPKI Bandung sebelum implementasi TRUST^{+} Posisitf.



Gambar 3.1. LAN Kantor BPPKI Bandung

Seperti terlihat pada skema LAN Kantor BPPKI Bandung, koneksi internet yang dibagikan pada komputer-komputer yang ada di LAN BPPKI Bandung (selanjutnya disebut LAN saja), melalui satu buat PC router dengan menggunakan sistem operasi Ubuntu 10.04 LTS Server. PC Router ini hanya berfungsi sebagai jalan keluar (*gateway)* bagi LAN untuk terkoneksi ke internet tanpa ada *software* tambahan seperti proxy server. Selain itu tidak ada pembatasan besarnya ukuran *file* yang diperbolehkan diunduh dari internet oleh komputer-komputer di LAN. Dengan kondisi PC Router ini sebagai *gateway* ke internet mengakibatkan beberapa kendala sebagai berikut :

1. *Bandwidth* koneksi ke internet bagi komputer-komputer di LAN akan saling berebut, sehingga bila ada komputer klien yang sedang mengunduh *file* yang besar dan mempegunakan software untuk mengakselerasi proses unduh, akan mempengaruhi kecepatan *bandwidth* bagi komputer klien lainnya di LAN.
2. Komputer-komputer klien di LAN akan terasa lambat mengakses ke internet karena untuk membuka sebuah situs web di internet harus *load* semua obyek-obyek halaman di situs tersebut termasuk obyek statis sepeti gambar latar halaman tersebut, dan obyek lainnya karena tidak ada proxy server yang berfungsi untuk melakukan *chacing* untuk menyimpan objek-objek Internet yang diminta (seperti halnya data/obyek di halaman situs web).
3. Situs-situs yang berbau pornografi yang sering membawa *spyware*, SARA, dan konten lainnya yang tidak sesuai dengan etika, akan dengan mudah diakses, dan menyebabkan kendala di LAN.
4. *Banner* atau iklan-iklan yang ada di suatu halaman situs web akan selalu terlihat, selain menghabiskan *bandwidth*, *banner* tersebut terkadang berisi iklan yang berbau pornografi.

3.2. Batasan Kebutuhan Untuk Implementasi TRUST^{+} Positif

Sesuai dengan kebijakan bahwa Balai Pengkajian dan Pengembangan Komunikasi dan Informatika (BPPKI) Bandung sebagai UPT dari Badan Penelitian dan Pengembangan SDM – Kemkominfo diharuskan menjadi *pilot*

project untuk menunjang upaya pemerintah dalam menerapkan program Internet Sehat dan Aman, dalam hal ini penerapan/implementasi Trust^{+} Positif di lingkungan kantor BPPKI Bandung dan Galeri Internet yang dikelola oleh BPPKI Bandung sebagai tempat layanan akses internet gratis yang diperuntukkan bagi kalangan pelajar, maka berikut adalah batasan kebutuhan untuk implementasinya :

1. Hak akses ke internet diperbolehkan bagi semua komputer klien yang ada di LAN Kantor BPPKI termasuk di dalamnya LAN Galeri Internet.
2. Situs-situs yang berbau pornografi yang sering membawa *spyware*, SARA, *banner*, dan konten lainnya yang tidak sesuai dengan etika akan diblok/tidak diperbolehkan diakses. Daftar situs-situs tersebut diambil dari kategori database yang dipakai dalam sistem TRUST^{+} Positif dimana database tersebut tersedia dan dapat diunduh di http://trustpositif.depkominfo.go.id.
3. Batasan-batasan pada no 2 berlaku pada semua komputer klien di LAN Kantor BPPKI Bandung tanpa terkecuali.

3.3. Implementasi TRUST^{+} Positif

3.3.1. Spesifikasi Hardware dan Software Digunakan

Berikut spesifikasi umum *hardware* dari komputer (PC Router) yang digunakan untuk implementasi TRUST^{+} Positif :

Tabel 3.1. Daftar *Hardware* Yang Digunakan Untuk Implementasi TRUST^{+} Positif

Hardware	Spesifikasi
Prosesor	1 Intel Xeon Processor 2,8 GHz
Memori	1 GB PC2100 DDR SDRAM running at 266MHz
Hardisk	36.4GB Wide Ultra320 SCSI 10,000 rpm
CD ROM Drive	48x IDE (ATAPI) CD-ROM Drive
Disk Drive	1.44 MB

Hardware	Spesifikasi
Kartu Grafis	Integrated ATI RAGE XL Video Controller with 8MB SDRAM Video Memory
Network Interface Card	1 x Network RJ-45 (Ethernet) built-in, 1x Network RJ-45 (Ethernet) PCI

PC-Router BPPKI Bandung yang telah ada (*existing*) menggunakan sistem operasi Ubuntu 10.04 LTS Server yang telah terkonfigurasi sebagai *router/gateway* internet dan sebagai *web server* lokal kantor BPPKI Bandung, sehingga dalam laporan kerja praktek ini tidak dibahas instalasi sistem operasi Ubuntu 10.04 LTS server dan konfigurasinya sebagai *router/gateway* dan *web server*.

3.3.2. Instalasi Dan Konfigurasi Squid Proxy Server

Pada sub bab ini akan dijelaskan cara instalasi *proxy server* Squid 2.7.STABLE7-1ubuntu12 (versi stabil terakhir untuk distro Ubuntu 10.04 pada saat server ini dibuat) dan konfigurasi dasar serta pengujiannya.

3.3.2.1. Instalasi Squid

Perintah unuk instalasi Squid adalah sebagai berikut, dengan asumsi komputer yang akan dipergunakan adalah komputer yang sama dengan komputer yang berfungsi sebagai router ke internet di BPPKI Bandung :

sudo apt-get install squid

```
dhiw@routerbox:~$ sudo apt-get install squid
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  squid-common squid-langpack
Suggested packages:
  squidclient squid-cgi logcheck-database resolvconf smbclient winbind
The following NEW packages will be installed:
  squid squid-common squid-langpack
0 upgraded, 3 newly installed, 0 to remove and 3 not upgraded.
Need to get 1,347kB of archives.
After this operation, 8,503kB of additional disk space will be used.
Do you want to continue [Y/n]? Y
Get:1 http://id.archive.ubuntu.com/ubuntu/ lucid/main squid-langpack 20100111-1 [228kB]
Get:2 http://id.archive.ubuntu.com/ubuntu/ lucid/main squid-common 2.7.STABLE7-
1ubuntu12 [353kB]
Get:3 http://id.archive.ubuntu.com/ubuntu/ lucid/main squid 2.7.STABLE7-1ubuntu12
[766kB]
Fetched 1,347kB in 21s (63.7kB/s)
Preconfiguring packages ...
Selecting previously deselected package squid-langpack.
(Reading database ... 47396 files and directories currently installed.)
Unpacking squid-langpack (from .../squid-langpack_20100111-1_all.deb) ...
Selecting previously deselected package squid-common.
Unpacking squid-common (from .../squid-common_2.7.STABLE7-1ubuntu12_all.deb) ...
Selecting previously deselected package squid.
Unpacking squid (from .../squid_2.7.STABLE7-1ubuntu12_i386.deb) ...
Processing triggers for ureadahead ...
Processing triggers for man-db ...
Setting up squid-langpack (20100111-1) ...
Setting up squid-common (2.7.STABLE7-1ubuntu12) ...

Setting up squid (2.7.STABLE7-1ubuntu12) ...
Creating squid spool directory structure
2011/01/10 21:08:20| Creating Swap Directories
```

Gambar 3.2. Instalasi Squid

Lokasi *file-file* penting dari Squid adalah sebagai berikut :

Tabel. 3.2. *File-File* Penting Squid

File	**Kegunaan**
/etc/squid/squid.conf	*File* konfigurasi Squid
/var/log/squid/access.log	*File* akses log dari Squid
/var/spool/squid	Direktori *cache* Squid secara *default*

Pengujian awal dilakukan untuk memeriksa apakah *service* Squid telah dijalankan atau tidak. Setelah proses instalasi Squid, secara otomatis Squid akan segera aktif, hal ini dapat diketahui dengan cara memberikan perintah:

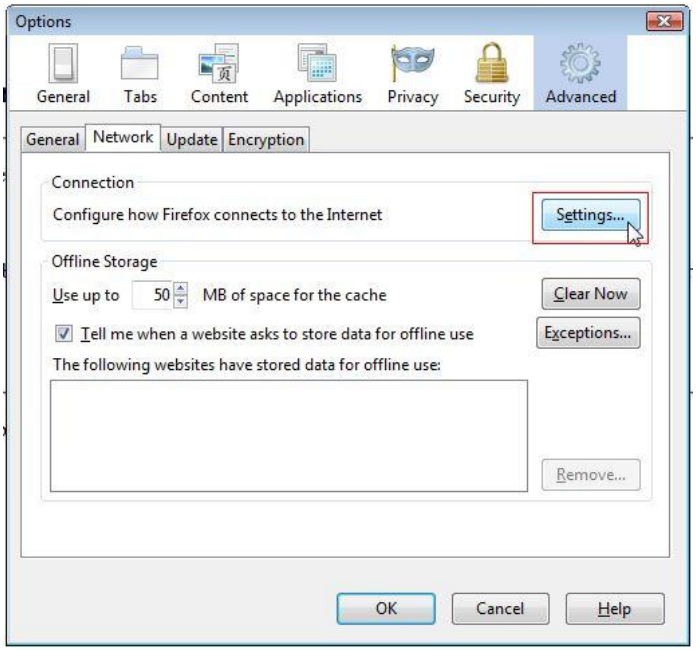
```
root@routerbox:/home/dhiw# ps ax |grep squid
        3935 ?       Ss     0:00 squid
        3937 ?       S      0:00 (squid)
```

Gambar 3.3. Pemeriksaan Service Squid

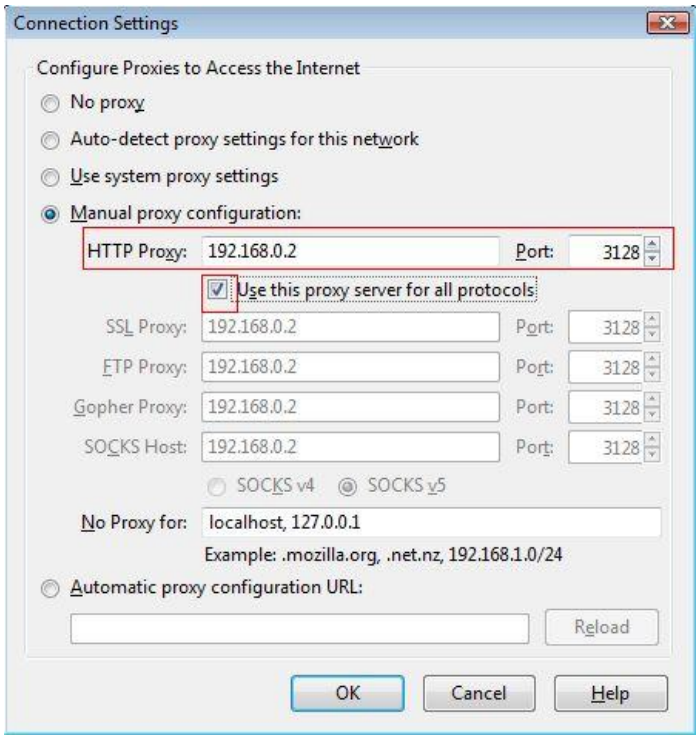
Dari hasil keluaran perintah tersebut terlihat bahwa Squid proxy server telah aktif pada PID 3935 (PID disini tidak sama untuk mesin-mesin yang lain tergantung banyaknya proses yang dilakukan oleh sebuah mesin/server). Tanpa konfigurasi awal secara *default* Squid sebenarnya sudah dapat digunakan, tetapi dengan keterbatasan dan tidak menjamin koneksi internet yang dilayani akan dilakukan dengan benar. Pengujian ini dilakukan hanya untuk melihat bekerja/tidaknya Squid proxy server yang dapat terlihat dari pengujian yang dilakukan di sisi server dan sisi klien.

Untuk pengujian di sisi klien dapat dilakukan dengan cara sebagai berikut:

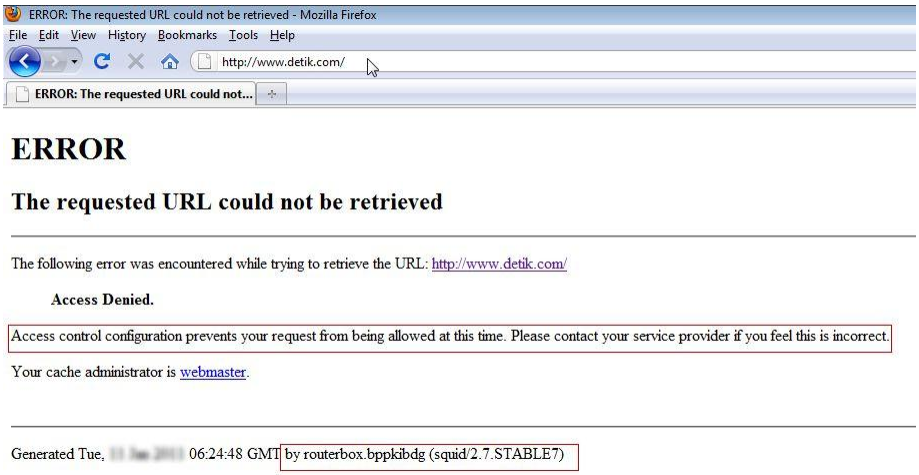
- Konfigurasi internet browser pada klien agar menggunakan proxy server yang telah dibuat sebelumnya yaitu dengan alamat : 192.168.0.2 pada port 3128 (*default port* yang digunakan oleh Squid) seperti terlihat pada gambar 3.3. Internet browser yang digunakan adalah Mozilla Firefox (konfigurasi pada internet browser lainnya dapat mengadaptasi konfigurasi *proxy setting* pada Mozilla Firefox ini), dengan memilih menu *Tools - Options – Advanced – Network – Setting* (gambar 3.4)
- Setelah konfigurasi selesai, uji pada internet browser dengan memasukkan URL suatu situs apa saja, misalnya : http://www.detik.com . Hasilnya seperti terlihat pada gambar 3.5 dimana terjadi *error* bahwa situs yang dituju tidak dapat dibuka karena aksesnya ditolak oleh Squid proxy server (routerbox.bppkibdg). Hal ini normal karena memang Squid belum terkonfigurasi, hanya dengan konfigurasi *default* saja.



Gambar 3.4. Menu Konfigurasi Mozilla Firefox



Gambar 3.5. Menu Konfigurasi Manual Proxy Pada Mozilla Firefox



Gambar 3.6. Pesan *Error* Pada Mozilla Firefox

Untuk pengujian di sisi server agar dapat diketahui ada/tidaknya permintaan dari klien tersebut dapat dengan cara sebagai berikut (pengujian di sisi server dilakukan untuk memonitor sebelum dan sesudah klien melakukan permintaan akses ke suatu situs) dengan perintah sebagai berikut :

tail –f /var/log/squid/access.log

```
root@routerbox:/home/dhiw# tail -f /var/log/squid/access.log
1294724158.594    0 192.168.0.22 TCP_DENIED/403 1511 GET http://google.co.id/ - NONE/- text/html
1294724159.167    0 192.168.0.22 TCP_DENIED/403 1511 GET http://google.co.id/ - NONE/- text/html
1294724159.642    0 192.168.0.22 TCP_DENIED/403 1511 GET http://google.co.id/ - NONE/- text/html
1294724160.266    0 192.168.0.22 TCP_DENIED/403 1511 GET http://google.co.id/ - NONE/- text/html
1294724161.970    0 192.168.0.22 TCP_DENIED/403 1511 GET http://google.co.id/ - NONE/- text/html
1294724185.689    0 192.168.0.22 TCP_DENIED/403 1511 GET http://google.co.id/ - NONE/- text/html
1294724561.035    0 192.168.0.22 TCP_DENIED/403 1515 CONNECT addons.mozilla.org:443 - NONE/- text/html
1294724561.064    0 192.168.0.22 TCP_DENIED/403 1511 CONNECT go.microsoft.com:443 - NONE/- text/html
1294724561.067    0 192.168.0.22 TCP_DENIED/403 1511 CONNECT aus2.mozilla.org:443 - NONE/- text/html
1294726021.813                0 192.168.0.22 TCP_DENIED/403 1595 POST
http://safebrowsing.clients.google.com/safebrowsing/downloads? - NONE/- text/html
1294727088.897    0 192.168.0.22 TCP_DENIED/403 1513 GET http://www.detik.com/ - NONE/- text/html
1294727088.976    0 192.168.0.22 TCP_DENIED/403 1535 GET http://www.detik.com/favicon.ico - NONE/-
text/html
1294727091.977    0 192.168.0.22 TCP_DENIED/403 1535 GET http://www.detik.com/favicon.ico - NONE/-
text/html
```

Gambar 3.7. *Log* Akses Klien terhadap Squid

Pada baris terakhir ouput perintah tersebut adalah permintaan terakhir dari klien terakhir terhadap Squid. Terlihat IP Address 192.168.0.22 (yang merupakan IP Address komputer klien yang digunakan untuk melakukan pengujian) dengan

kondisi akses TCP ditolak (*TCP_Denied)* terhadap situs http://www.detik.com dengan kode *error* 403 (*The requested URL could not be retrieved*). Hal ini menunjukkan adanya aktivitas Squid yang sudah dapat menerima permintaan dari klien.

Untuk menghentikan Squid, dilakukan dengan memberikan perintah sebagai berikut (dengan menggunakan *user* root) :

squid –k kill

pastikan squid telah berhenti dengan perintah **ps ax |grep squid** seperti telah dijelaskan sebelumnya. Sedangkan untuk mengaktifkan kembali Squid dilakukan dengan perintah sebagai berikut :

squid start

3.3.2.2. Konfigurasi Squid

Konfigurasi Squid pertama adalah membuat direktori cache dimana *default* dari instalasi Squid pertama kali adalah di direktori */var/spool/squ*id. Letak direktori cache ini akan dipindahkan ke direktori */cache* dengan pertimbangan kapasitas direktori */cache* telah dialokasikan sebelumnya sebesar 15GB di partisi hardisk tersendiri.

```
root@routerbox:/home/dhiw# df -h
Filesystem          Size  Used Avail Use% Mounted on
/dev/sda1           4.6G  817M  3.6G  19% /
none                496M  180K  496M   1% /dev
none                501M  4.0K  501M   1% /dev/shm
none                501M   52K  501M   1% /var/run
none                501M     0  501M   0% /var/lock
none                501M     0  501M   0% /lib/init/rw
/dev/sda8            15G  164M   14G   2% /cache
/dev/sda6           9.2G  150M  8.6G   2% /home
/dev/sda5           4.6G  304M  4.1G   7% /var
/home/dhiw/.Private  9.2G  150M  8.6G   2% /home/dhiw
```

Gambar 3.8. Alolasi Kapasitas Partisi Hardisk

Ubah kepemilikan direktori /*cache* menjadi milik *user* Squid dalam hal ini nama *user*-nya adalah **proxy** dengan perintah (dengan menggunakan *user* root) :

chown -Rf proxy:proxy /cache/

Kemudian konfigurasi Squid dengan menyunting *file* konfigurasi Squid berada di */etc/squid/squid.conf*. *File* tersebut akan disunting dengan penyunting yang tersedia (penulis menggunakan *mcedit/joe* sebagai aplikasi penyuntingnya). Sebagai *backup* dibuat *file* salinan sebelum merubah isi *file* konfigurasi tersebut misalnya dengan nama *squid.conf.original* pada direktori */etc/squid/* juga.

File konfigurasi Squid ini terdiri atas ribuan baris dan dipisahkan menjadi beberapa bagian menurut fungsinya masing-masing. Tetapi tidak semua baris akan di-*load* oleh Squid Proxy Server, hanya baris-baris *file* konfigurasi yang **tidak diberi tanda "#"** (tanda dimana menunjukkan bahwa baris setelah tanda # hanya sebagai komentar saja). Untuk memudahkan dalam penyuntingan *file* konfigurasi ini telah dimodifikasi dengan menghapus baris-baris yang tidak dipergunakan dan hanya menyisakan baris-baris konfigurasi (*tag*) yang secara *default* memang dipergunakan Squid. Sebagian *tag* dalam *file* konfigurasi ini adalah *tag* yang merupakan nilai awal dari *file* konfigurasi asli yang di-*load* oleh Squid. Untuk membedakan *tag* yang ditambahkan atau dimodifikasi, akan diberi warna merah sebagai tanda pada baris yang dimaksud. Berikut adalah isi dari *file* ***/etc/squid/squid.conf*** yang telah disunting :

```
#         WELCOME TO SQUID 2.7.STABLE7
#         ----------------------------
#
#--------------------------------------
#            ACCESS CONTROLS
#--------------------------------------
# (TAG : acl ) Mendefinisikan daftar akses
# berikut ini adalah daftar akses default
#
acl all src all
acl manager proto cache_object
acl localhost src 127.0.0.1/32
acl to_localhost dst 127.0.0.0/8 0.0.0.0/32
acl localnet src 192.168.0.0/24        #mendefinisikan LAN BPPKI Bandung
```

```
#
#berikut ini adalah daftar akses default untuk port yang digunakan di internet
acl SSL_ports port 443          # https
acl SSL_ports port 563          # snews
acl SSL_ports port 873          # rsync
acl Safe_ports port 80          # http
acl Safe_ports port 21          # ftp
acl Safe_ports port 443         # https
acl Safe_ports port 70          # gopher
acl Safe_ports port 210         # wais
acl Safe_ports port 1025-65535  # unregistered ports
acl Safe_ports port 280         # http-mgmt
acl Safe_ports port 488         # gss-http
acl Safe_ports port 591         # filemaker
acl Safe_ports port 777         # multiling http
acl Safe_ports port 631         # cups
acl Safe_ports port 873         # rsync
acl Safe_ports port 901         # SWAT
acl purge method PURGE
acl CONNECT method CONNECT
#
#
# (TAG : http_access)
# Mendefinisikan hak akses dari daftar akses yang
# telah didefinisikan di tag acl list
#-----------------------------------------------
#
http_access allow manager localhost
http_access deny manager
http_access allow purge localhost
http_access deny purge
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access deny to_localhost
#memperbolehkan LAN BPPKI Bandung mengakses internet melalui proxy
http_access allow localnet
http_access allow localhost
http_access deny all
#
#
# (TAG : icp_access)
# Konfigurasi untuk koneksi dengan proxy lainnya
# tetapi hanya dari LAN saja
#-----------------------------------------------
#
icp_access allow localnet
icp_access deny all
#
```

#---
NETWORK OPTIONS
#---
(TAG : http_port)
Konfigurasi untuk port yang dialokasikan untuk
squid dapat mendengar TCP request dari klien
#
http_port 3128
#
#
#---
OPTIONS WHICH AFFECT THE NEIGHBOR SELECTION ALGORITHM
#---
(TAG: hierarchy_stoplist)
dugunakan untuk opsi agar squid tidak melakukan query
dari proxy lain untuk beberapa obyek.
#---
hierarchy_stoplist cgi-bin ?
#
#
#---
MEMORY CHACE OPTIONS
#---
#(TAG: cache_mem)
opsi untuk alokasi memori yang nantinya akan
#dipergunakan oleh : In-TRAnsits objects, Hot-Objects
dan negative-cached objects. Contoh : 128 MB berarti memori fisik yang
#dipakai untuk keperluan cache sebesar 128 MB
#
(TAG : maximum_object_size_in_memory) untuk membatasi ukuran
#maksismum cache yang akan ditampung sementara di memori fisik. Contoh :
#128 KB berarti ukuran file yang di-cache di memori fisik maksimum 128 KB
#---
cache_mem 128 MB
maximum_object_size_in_memory 128 KB
#
#---
DISK CACHE OPTIONS
#---
cache_dir aufs /cache 5120 16 256
minimum_object_size 0 KB
maximum_object_size 32 MB
cache_swap_low 90
cache_swap_high 95

#(TAG: cache_dir)
direktori/partisi HDD yang dipergunakan untuk menyimpan
obyek-obyek yang telah di-cache pada partisi dengan akses ufs

```
# dan ukuran HDD yang akan  digunakan  :
# /cache 5120 16 256 artinya kapasitas HDD yang digunakan pada direktori
# /cache adalah sebesar sebesar 5120 KB dengan di dalamnya akan dibuat
#sebanyak 16 direktori dan 256 sub direktori di bawah 16 direktori utama tadi,
#tempat untuk menyimpan obyek-obyek yang telah di-cache
#
#TAG: minimun_object_size dan  maximum_object_size adalah untuk pengaturan
#besarnya file dari obyek-obyek yang disimpan, bila lebih dari yang terdefinisi
#maka tidak akan disimpan sebagai cache.
#
#TAG: cache_swap_low dan cache_swap_high adalah untuk mendefinisikan
melakukan swap bila mencapai nilai yang ditentukan (dalam prosentase)
#-----------------------------------------------------
#
#-----------------------------------------------------
#             LOG FILE OPTIONS
#-----------------------------------------------------
#
access_log /var/log/squid/access.log squid
#
#-----------------------------------------------------
#            OPTIONS FOR URL REWRITING
#-----------------------------------------------------
# untuk aktivasi squidguard
#-------------------------
#
url_rewrite_program /usr/bin/squidGuard
#
#-----------------------------------------------------
#            OPTIONS FOR TUNING THE CACHE
#-----------------------------------------------------
refresh_pattern ^ftp: 1440 20% 10080
refresh_pattern ^gopher: 1440 0% 1440
refresh_pattern -i (/cgi-bin/|\?) 0 0% 0
refresh_pattern (Release|Package(.gz)*)$      0          20%     2880
refresh_pattern (\.deb|\.udeb)$   129600 100% 129600
refresh_pattern . 0 20% 4320
#
#-----------------------------------------------------
#                    HTTP OPTIONS
#-----------------------------------------------------
acl shoutcast rep_header X-HTTP09-First-Line ^ICY.[0-9]
upgrade_http0.9 deny shoutcast
acl apache rep_header Server ^Apache
broken_vary_encoding allow apache
extension_methods REPORT MERGE MKACTIVITY CHECKOUT
#
#-----------------------------------------------------
```

```
#                ADMINISTRATIVE PARAMETERS
#------------------------------------------------------
#untuk menghubungi email dari adminstrator proxy server ini
#
cache_mgr widdie@budhiarta.web.id
#
#------------------------------------------------------
#                     DNS OPTIONS
#------------------------------------------------------
hosts_file /etc/hosts
#
#------------------------------------------------------
# MISCELLANEOUS
#------------------------------------------------------
coredump_dir /var/spool/squid

#EOF
```

Setelah *file* **/etc/squid/squid.conf** tersebut selesai disunting, agar konfigurasi yang baru diterapkan oleh Squid maka, Squid harus di-*restart*. Sebelumnya dipastikan dahulu ada/tidak ada kesalahan dalam penulisannya, dapat digunakan perintah sebagai berikut (menggunakan *user* root) setelah sebelumnya Squid dihentikan terlebih dahulu :

squid –k parse

Bila tidak ada kesalahan dalam penulisan *file* konfigurasi Squid maka tidak akan muncul pesan apa-apa, tetapi bila terdapat kesalahan akan ditampilkan informasi kesalahan pada baris kesekian sesuai dengan kesalahan yang terjadi.Setelah dipastikan tidak ada kesalahan dalam *file* konfigurasi Squid dapat kembali diaktfikan.

Sebelum Squid diaktifkan, karena dalam file konfigurasi telah diubah lokasi direktori tempat menyimpan *cache objects* ke direktori **/cache** maka struktur direktori tempat *cache objects* harus dibuat kembali dengan perintah :

s**quid –z**

Pengujian konfigurasi ini seperti telah dijelaskan sebelumnya dengan melihat *file* **/var/log/squid/access.log** pada saat klien mengakses internet,

misalnya mengakses situs http://www.unikom.ac.id , maka di *file* access.log akan tercatat. Hal ini menunjukkan bahwa konfigurasi awal Squid telah berhasil dilakukan.

```
root@routerbox:/home/dhiw# tail -f /var/log/squid/access.log
1296150382.228    17 192.168.0.22 TCP_REFRESH_HIT/304 410 GET
http://www.unikom.ac.id/image/img_slide/img13.jpg - DIRECT/222.124.203.55 -
1296150387.226    19 192.168.0.22 TCP_REFRESH_HIT/304 292 GET
http://www.unikom.ac.id/image/img_slide/img14.jpg - DIRECT/222.124.203.55 -
1296150392.223    15 192.168.0.22 TCP_REFRESH_HIT/304 292 GET
http://www.unikom.ac.id/image/img_slide/img8.jpg - DIRECT/222.124.203.55 -
1296150397.231    20 192.168.0.22 TCP_REFRESH_HIT/304 410 GET
http://www.unikom.ac.id/image/img_slide/img9.jpg - DIRECT/222.124.203.55 -
1296150402.232    18 192.168.0.22 TCP_REFRESH_HIT/304 291 GET
http://www.unikom.ac.id/image/img_slide/img10.jpg - DIRECT/222.124.203.55 -
1296150407.230    15 192.168.0.22 TCP_REFRESH_HIT/304 410 GET
http://www.unikom.ac.id/image/img_slide/img11.jpg - DIRECT/222.124.203.55 -
1296150412.234    18 192.168.0.22 TCP_REFRESH_HIT/304 411 GET
http://www.unikom.ac.id/image/img_slide/img12.jpg - DIRECT/222.124.203.55 -
```

Gambar 3.9. Pengujian Squid Pada Sisi Server

3.3.3. Instalasi Dan Konfigurasi SquidGuard

Untuk mengakomodir batasan kebutuhan implementasi TRUST^{+} Positif yaitu memblokir situs-situs yang berbau pornografi yang sering membawa *spyware*, SARA, dan konten lainnya yang tidak sesuai dengan etika akan diblok/tidak diperbolehkan diakses, digunakan SquidGuard.

SquidGuard bertindak sebagai program *redirector*/penyedia *database* situs-situs yang akan diblokir dan dapat diintegrasikan dengan Squid. SquidGuard akan membaca daftar situs-situs yang telah disediakan dan selanjutnya akan memberikan aturan-aturan terhadap setiap situs yang ada dalam *database*, apakah diperbolehkan diakses/tidak diperkenankan diakses. Daftar situs-situs tersebut diambil dari kategori *database* yang dipakai dalam sistem TRUST^{+} Positif.

Database tersebut tersedia dan dapat diunduh di http://trustpositif.depkominfo.go.id .

3.3.3.1. Instalasi SquidGuard

SquidGuard yang digunakan adalah SquidGuard: 1.2.0 Berkeley DB 4.8.24: (August 14, 2009). Perintah untuk melakukan instalasi SquidGuard adalah sebagai berikut (menggunakan user *root*) :

sudo apt-get install squidguard

```
root@routerbox:/etc/squid# apt-get install squidguard
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
  chastity-list
The following NEW packages will be installed:
  squidguard
0 upgraded, 1 newly installed, 0 to remove and 27 not upgraded.
Need to get 137kB of archives.
After this operation, 459kB of additional disk space will be used.
Get:1 http://id.archive.ubuntu.com/ubuntu/ lucid-updates/universe squidgua
rd 1.2.0-8.4ubuntu1.0.10.04.1 [137kB]
Fetched 137kB in 2s (46.0kB/s)
Preconfiguring packages ...
Selecting previously deselected package squidguard.
(Reading database ... 49160 files and directories currently installed.)
Unpacking squidguard (from .../squidguard_1.2.0-8.4ubuntu1.0.10.04.1_i386.
deb) ...
Processing triggers for man-db ...
Setting up squidguard (1.2.0-8.4ubuntu1.0.10.04.1) ...
Double checking directory and file permissions...done!
Re-building SquidGuard db files...done!
Reloading Squid...done!
```

Gambar 3.10. Instalasi SquidGuard

Tabel. 3.3. *File-file* Penting SquidGuard

File	**Kegunaan**
/etc/squid/squidGuard.conf	*File* konfigurasi SquidGuard
/var/log/squid/squidGuard.log	*File* akses log dari SquidGuard
/var/lib/squidguard/db	*File* Database SquidGuard

Setelah instalasi SquidGuard selesai, hak akses direktori *log* untuk SquidGuard diubah menjadi milik *user proxy* dan *group proxy* (*user* dan *group* untuk Squid *Proxy Server*) dengan perintah (menggunakan *user root*) :

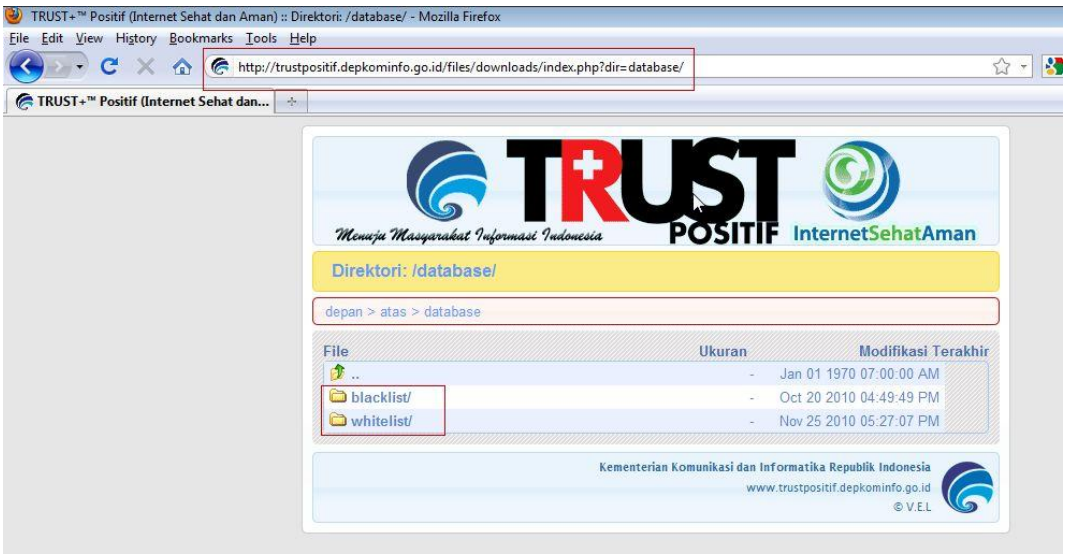
chown proxy.proxy /var/log/squid/squigguard –Rf

Hal ini dimaksudkan agar Squid dapat menuliskan *log* aktivitas antara Squid dan SquidGuard.

3.3.3.2. Database TRUST+ Positif

Sebelum menyunting *file* konfigurasi SquidGuard, perlu diketahui terlebih dahulu kategori-kategori *database* dari situs-situs yang akan digunakan oleh SquidGuard, dalam hal ini kategori-kategori tesebut diunduh dari situs TRUST+ Positif berupa *file* yang isinya adalah data raw masing-masing kategori :

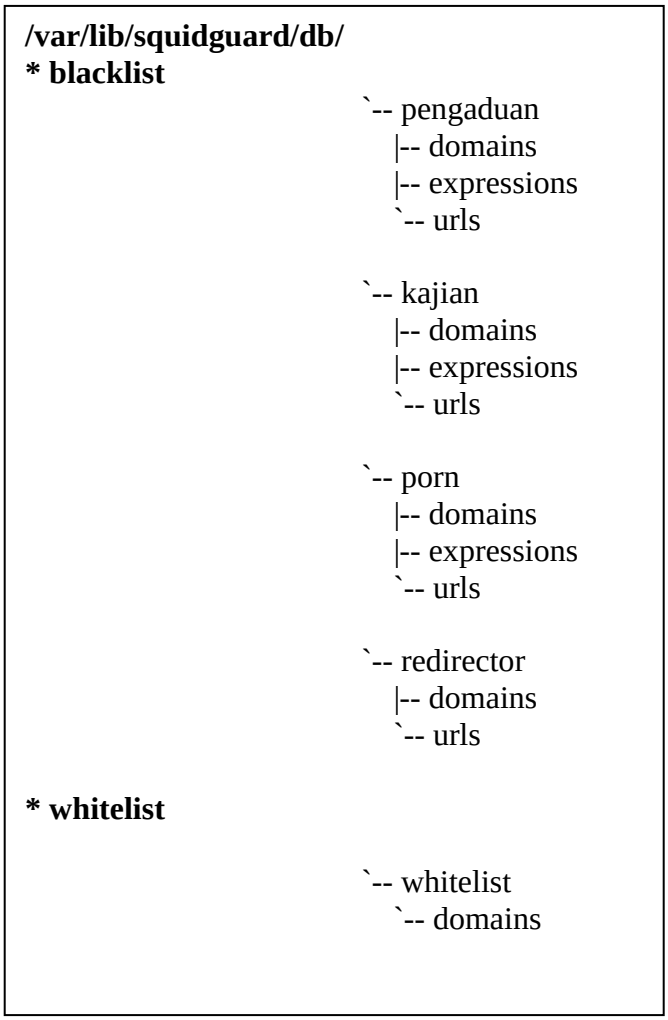
http://trustpositif.depkominfo.go.id/files/downloads/index.php?dir=database/



Gambar 3.11. Tampilan Halaman Unduh TRUST+ Positif

Di situs tersebut ada 2 bagian *database* (dalam 2 direktori utama) yaitu bagian Daftar Hitam/*Blacklist* dan Daftar Putih/*whitelist*. Masing-masing bagian mempunyai kategori (direktori) dan jenis *database* seperti telah dijelaskan pada sub bab 2.2.1.2. Masing-masing direktori mempunyai sub direktori dan terdapat *file-file* berisi daftar domain (*file* : ***domains***), daftar URL (*file* : *urls*), dan daftar *keyword* (*file* : ***expressions***).

Struktur Directory pada kategori Database setelah diunduh dan disimpan di dalam *folder* **/var/lib/squidguard/db/** :



Gambar 3.12. Struktur Directori Pada Kategori *Database* Squidguard

Informasi Data File pada kategori Database:

- domains: data mentah (raw) dari daftar Top-Level Domain
- urls: data mentah (raw) dari daftar URL
- expressions: data matang (raw) dari daftar Ekspresi/Keyword dalam bentuk regular expression

3.3.3.3. Konfigurasi SquidGuard

File konfigurasi SquidGuard berada di direktori **/etc/squid/squidGuard.conf**. Berikut adalah isi *file* tersebut :

```
#
# CONFIG FILE FOR SQUIDGUARD
#

dbhome /var/lib/squidguard/db
logdir /var/log/squid

#
# TIME RULES:
# abbrev for weekdays:
# s = sun, m = mon, t =tue, w = wed, h = thu, f = fri, a = sat

time workhours {
        weekly mtwhf 08:00 - 16:30
}

source localnet {
        ip 192.168.0.0/24
}
dest whitelist {
        domainlist whitelist/domains
}
dest adv {
        domainlist adv/domains
        urllist adv/urls
}
dest pengaduan {
        domainlist pengaduan/domains
        urllist pengaduan/urls
        expressionlist pengaduan/expressions
}
dest kajian {
        domainlist kajian/domains
        urllist kajian/urls
        expressionlist kajian/expressions
}
dest porn {
        domainlist porn/domains
        urllist porn/urls
        expressionlist porn/expressions
}
dest redirector {
```

```
        domainlist redirector/domains
        urllist redirector/urls
}

acl {
        privileged {
                pass whitelist !adv any
        }

        localnet within workhours {
                pass whitelist !workhours !adv !pengaduan !kajian !porn
!redirector any
        } else {
                pass whitelist !adv !pengaduan !kajian !porn !redirector any
        }

default {
                pass whitelist !adv !pengaduan !kajian !porn !redirector all
                redirect http://192.168.0.2/image/blocked.png
        }
```

Keterangan konfigurasi :

1. Tag **dbhome** merupakan tag yang menunjukkan letak direktori database SquidGuard, dalam konfigurasi ini berada di : **/var/lib/squidguard/db.**
2. Tag **logdir** merupakan tag yang menunjukkan letak direktori log dari Squid, dalam konfigurasi ini berada di : **/var/log/squid.**
3. Tag **time,** merupakan tag untuk mendefinisikan aturan waktu kapan saja SquidGuard akan dijalankan. Dalam konfigurasi ini didefinisikan aturan bernama "wokhours"' dengan aturan **mtwhf 08:00 - 16:30** yang berarti "workhours" berlaku setiap hari Senin sampai dengan Jumat mulai pukul 08:00 dan berakhir pukul 16:00
4. Tag **dest** menunjukkan pendefinisian kategori yang akan diblok (sesuai dengan kategori-kategori TRUST^{+} Positif yang sebelumnya telah dijelaskan). Dalam tag ini dapat dimasukan **domainlist** yang merujuk ke *file* **domains** (berisi nama-nama domain yang akan diblok/tidak) yang berada di direktori berdasarkan pendefinisian kategori di tag **dest**. Contoh : "**dest kajian"** dengan isi "**domainlist kajian/domains"** menunjukkan bahwa dalam kategori **kajian** daftar nama domain yang akan diblok/tidak

ada di *file* **/var/lib/squidguard/db/kajian/domains.** Begitu uga berlaku untuk **"urlist"** dan **"expressinslist"**.

5. Tag **acl** merupakan pendefinisian aktual suatu kategori diblok atau tidak. Dengan memberi nama definisi aktual dapat diterapkan aturan-aturan pemblokiran. Contoh :

```
default {
pass whitelist !adv !pengaduan !kajian !porn !redirector all
redirect http://192.168.0.2/image/blocked.png
}
```

Menunjukkan bahwa secara **default** semua klien (**all**) diberi aturan diperbolehkan (**pass**) mengakes situs-situs yang ada di daftar **whitelist** tetapi tidak diperbolehkan (dengan memberi karakter "**!**" pada kategori yang akan diberi aturan tidak diperbolehkan) mengakses situs-situs yang ada di daftar **adv, pengaduan, kajian, porn, redirector**. Bila klien tetap mengakses situs-situs yang tidak diperbolehkan, maka *internet browser* di klien akan diarahkan ke **http://192.168.0.2/image/blocked.png** yaitu webserver lokal (IP dari webserver) dan memunculkan gambar **blocked.png** seperti pada gambar di bawan ini :



Gambar 3.13. Blocked.png

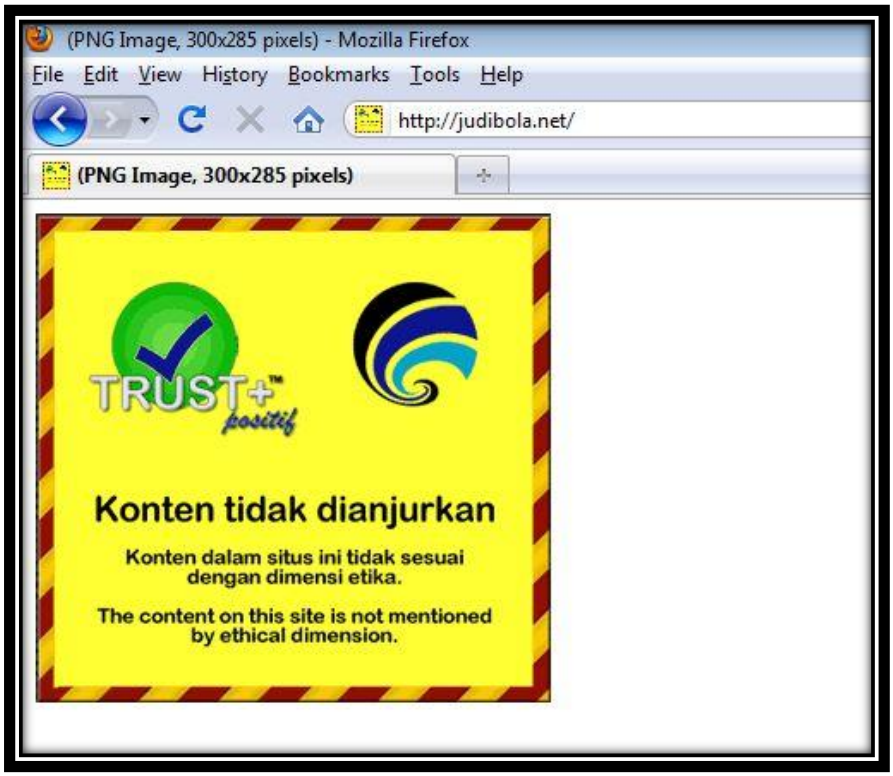
Hal-hal yang perlu diperhatikan untuk konfigurasi SquidGuard :

1. Perlu diperhatikan bahwa baris pertama dari *file* konfigurasi **/etc/squid/squidGuard.conf** , **tidak boleh berupa baris kosong.** Bila merupakan baris kosong maka akan menyebabkan SquidGuard gagal dieksekusi.
2. Sebelum menjalankan SquidGuard, untuk mengkonversi data *file pada* database TRUST^{+} Positif (SquidGuard) yang masih berupa teks menjadi format *file DB* untuk SquidGuard, dengan perintah sebagai berikut :

   squidguard –C all

   kemudian pastikan *user squid (proxy)* dan ***group proxy*** mempunyai hak akses pada database SquidGuard dengan perintah :

   chown –R proxy:proxy /var/lib/squidguard/db/*
3. Untuk pengujian di sisi klien dapat dicoba dengan mengakases salah satu situs yang terdaftar misalnya di daftar **kajian** dengan melihat isi **file** domains di direktori **/var/lib/squidguard/db/kajian/.** Sebagai contoh : http://judibola.net bila dicoba diakses di klien, maka klien tersebut akan diarahkan membuka **http://192.168.0.2/image/blocked.png.**



Gambar 3.14. Contoh Situs Web Yang Terblokir Oleh SquidGuard

3.3.4. Proxy Tansparan

Agar klien yang berada di LAN BPPKI Bandung dapat diatur akses ke situs-situs web yang konten-kontennya tidak diperbolehkan, maka klien harus diarahkan agar aksesnya harus melalui *Squid Proxy Server*. Pengaturan pada sisi klien telah dijelaskan pada sub bab 3.3.2.1. Instalasi Squid. Dengan cara demikian tentunya akses ke internet dari klien akan melewati *Squid Proxy Server* terlebih dahulu, tetapi apabila di sisi klien tidak dilakukan pengaturan tersebut (pada pilihan di *browser internet* diatur menjadi "*no proxy*" atau tidak menggunakan proxy server, maka klien dapat mengakses situs-situs yang seharusnya terblokir.

Dari sini akan timbul suatu permasalahan dimana untuk mengkonfigurasi *internet browser* masing-masing klien tentunya akan memakan waktu dan tenaga ekstra seorang administrator, terlebih apabila jumlah komputer klien sangat banyak. Untuk mengatasi permasalahan tersebut maka dilakukan konfigurasi ulang agar Squid dapat berfungsi sebagai *proxy* transparan; yaitu *proxy server* yang dapat mengarahkan secara keseluruhan akses intenet setiap klien di suatu LAN agar selalu melewati *proxy server*. Berikut ini langkah konfigurasi agar dapat membuat Squid menjadi *proxy* transparan :

1. Pada *file* konfigurasi Squid **/etc/squid/squid.conf** sunting *TAG :* **http_port** yang awalnya bernilai "**http_port 3128**" menjadi **http_port 3128 transparent**" . Hal ini agar Squid secara otomatis mengaktifkan konfigurasi internalnya agar Squid dapat berlaku sebagai *proxy* transparan.
2. Karena Squid sebagai proxy server ter-*install* dalam satu komputer yang sama dengan komputer router dari LAN BPPKI Bandung, maka perlu dikonfigurasi ulang agar router tersebut dapat mengatur apabila ada permintaan akses ke internet (TCP port 80; akses ke situs web) dari semua klien yang ada di LAN BPPKI Bandung, maka permintaan tersebut diarahkan ulang ke Squid sebagai *proxy server* pada port 3128, sebelum diperbolehkan mengakses situs yang bersangkutan. Pengaturan yang dilakukan adalah pengaturan terhadap aturan *firewall* dari router dengan perintah sebagai berikut :

   iptables -A PREROUTING -t nat -p tcp --dport 80 -j REDIRECT --to-port 3128