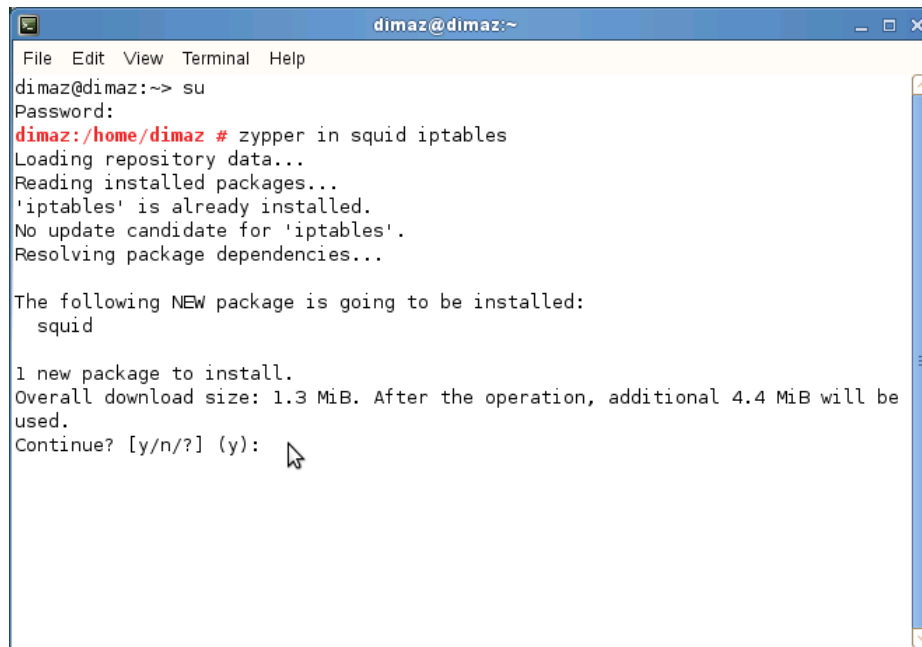


Konfigurasi dasar Squid Proxy+Gateway Server di SLES 11

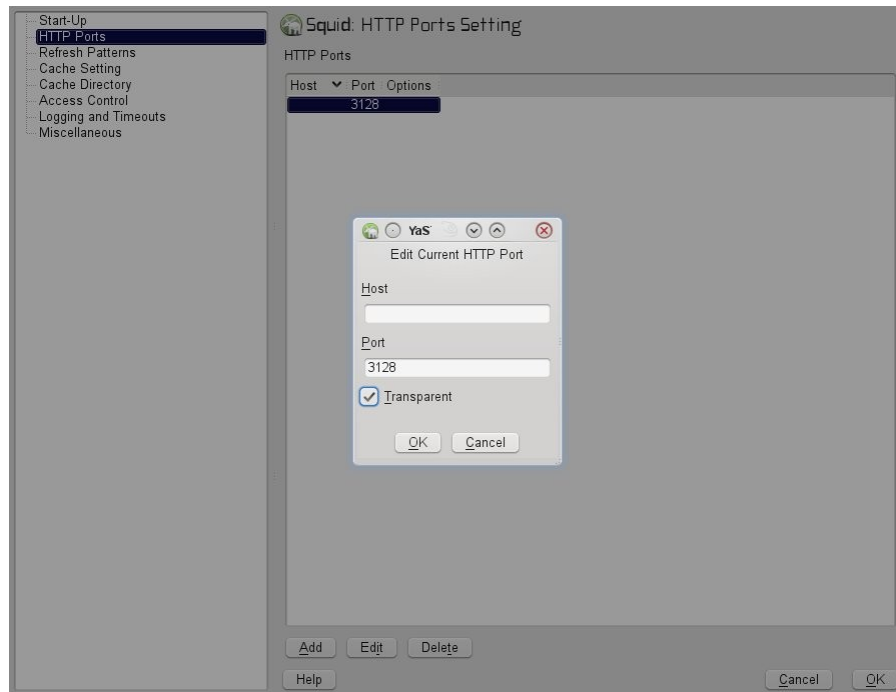
Proxy server berfungsi tidak hanya sebagai server penyimpanan sementara dari request-request ke internet sehingga ketika kita mengakses web yang sama dari komputer lain akan terasa lebih cepat, tapi dapat berfungsi juga sebagai filterisasi/blocking situs atau url. ibarat orang, udah kaya satpam aja . :D

Aplikasi Proxy server yang cukup terkenal dan handal yaitu Squid Proxy, tutorial ini menjelaskan bagaimana konfigurasi squid di SLES 11 SP1. (dengan catatan, PC server memiliki 2 buah NIC untuk melakukan routing, sehingga PC server juga bekerja sebagai Gateway)



```
dimaz@dimaz:~  
File Edit View Terminal Help  
dimaz@dimaz:~> su  
Password:  
dimaz:/home/dimaz # zypper in squid iptables  
Loading repository data...  
Reading installed packages...  
'iptables' is already installed.  
No update candidate for 'iptables'.  
Resolving package dependencies...  
  
The following NEW package is going to be installed:  
  squid  
  
1 new package to install.  
Overall download size: 1.3 MiB. After the operation, additional 4.4 MiB will be used.  
Continue? [y/n/?] (y):
```

- Install squid proxy dan iptables pada **gnome-terminal** dengan menggunakan perintah **# zypper in squid iptables**
- kemudian jalankan **YaST – Squid** dari **gnome-terminal** dengan perintah **# yast2 squid**



- klik **HTTP Ports** kemudian klik **edit**, lalu ceklist **Transparent**, lalu klik **OK**
- kemudian edit file konfigurasi squid untuk menambahkan acl dengan perintah **# vi /etc/squid/squid.conf**

```
File Edit View Scrollback Bookmarks Settings Help
acl localnet src 10.0.0.0/8
acl localnet src 172.16.0.0/12
acl localnet src 192.168.0.0/16
acl SSL_ports port 443
acl Safe_ports port 80
acl Safe_ports port 21
acl Safe_ports port 443
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
acl shoutcast rep_header X-HTTP09-First-Line ^ICY:[0-9]
acl apache rep_header Server ^Apache
acl domain dstdomain "/etc/squid/domain.txt"
acl url url_regex -i "/etc/squid/url.txt"
acl waktu time MTWHFAS 07:00-17:00

# TAG: cache
# A list of ACL elements which, if matched, cause the request to
# not be satisfied from the cache and the reply to not be cached.
# In other words, use this to force certain objects to never be cached.
#
-- INSERT --                                     636,1      12%
```

- kemudian tambahkan line ACL dibawah untuk menentukan peraturan berdasarkan domain, waktu, dan URL
acl domain dstdomain “/etc/squid/domain.txt”
(menentukan domain dari sebuah file)
acl url url_regex -i “/etc/squid/url.txt”
(menentukan URL dari sebuah file)
acl waktu time MTWHFAS 07:00-17:00
(menentukan hari dan jam, M = monday T = Tuesday W = Wednesday H = Thursday F = Friday A = Saturday S = Sunday)

```
File Edit View Scrollback Bookmarks Settings Help
#Default:
# http_access deny all
#
#Recommended minimum configuration:
#
# Only allow cachemgr access from localhost
# Deny requests to unknown ports
# Deny CONNECT to other than SSL ports
# 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
# And finally deny all other access to this proxy
http_access deny domain waktu
http_access deny url
http_access allow manager localhost
http_access deny manager
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localnet
http_access allow localhost
http_access deny all

#
# We strongly recommend the following be uncommented to protect innocent
# web applications running on the proxy server who think the only
# one who can access services on "localhost" is a local user
-- REPLACE --
```

- lalu tambahkan juga line dibawah untuk menentukan ACL tersebut di blok atau di izinkan
 - http_access deny domain waktu** = memblok domain-domain yang sudah ditentukan pada waktu yang sudah ditentukan.
 - http_access deny url** = memblok kata-kata yang sudah ditentukan pada saat menggunakan search engine, contoh : google.com

```
File Edit View Scrollback Bookmarks Settings Help
www.facebook.com
www.youtube.com
~
```

- lalu save file konfigurasi squid.conf, kemudian buat file domain.txt didalam direktori /etc/squid/ dengan perintah # **touch /etc/squid/domain.txt** lalu edit file domain.txt # **vi /etc/squid/domain.txt** lalu tambahkan nama-nama domain yang akan di blok, contoh : www.facebook.com, www.youtube.com lalu save file tersebut
-

```
File Edit View Scrollback Bookmarks Settings Help
xxx
porno
3gp
~
~
```

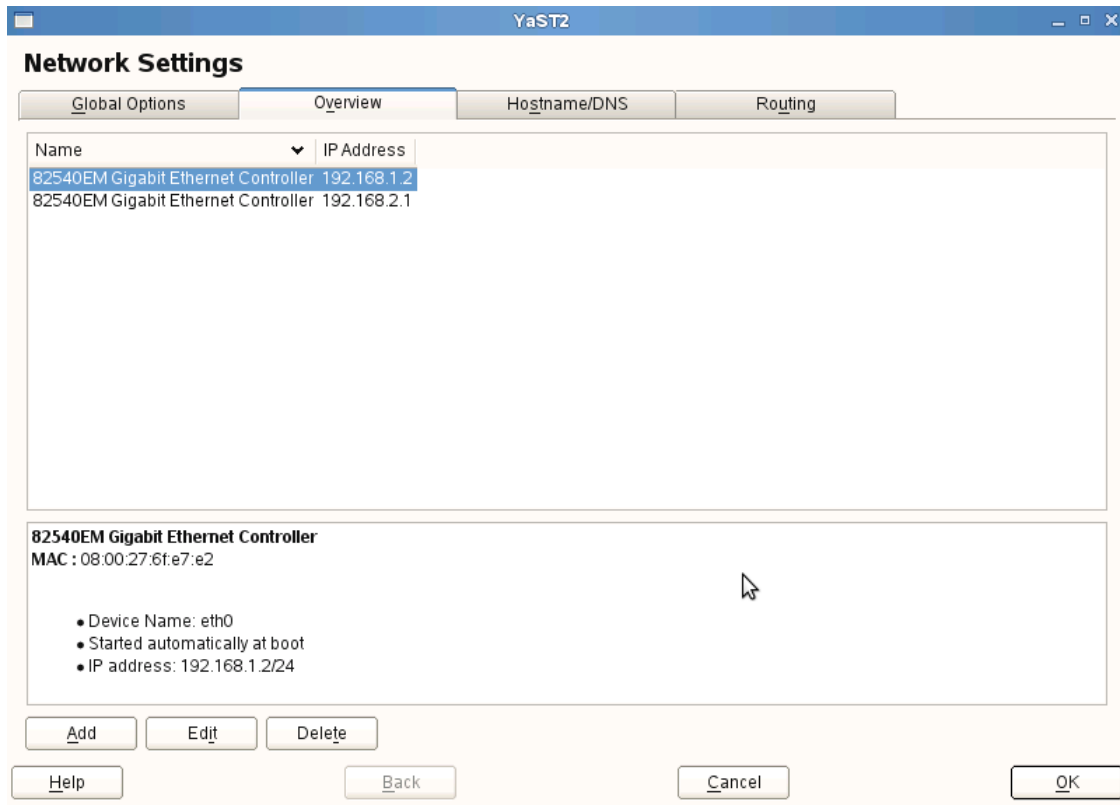
- kemudian buat file /etc/squid/url.txt dengan perintah # **touch /etc/squid/url.txt** lalu edit file tersebut lalu tambahkan kata-kata/url yang ingin diblok seperti gambar dibawah lalu save file tersebut.

```
File Edit View Scrollback Bookmarks Settings Help
dimaz@dimaz:~> su
Password:
dimaz:/home/dimaz # vi /etc/squid/squid.conf
dimaz:/home/dimaz # touch /etc/squid/domain.txt
dimaz:/home/dimaz # vi /etc/squid/domain.txt
dimaz:/home/dimaz # touch /etc/squid/url.txt
dimaz:/home/dimaz # vi /etc/squid/url.txt
dimaz:/home/dimaz # rcsquid start
Starting WWW-proxy squid - Warning: squid already running !           failed
dimaz:/home/dimaz # rcsquid restart
Shutting down WWW-proxy squid                                         done
Starting WWW-proxy squid                                             done
dimaz:/home/dimaz # █
```

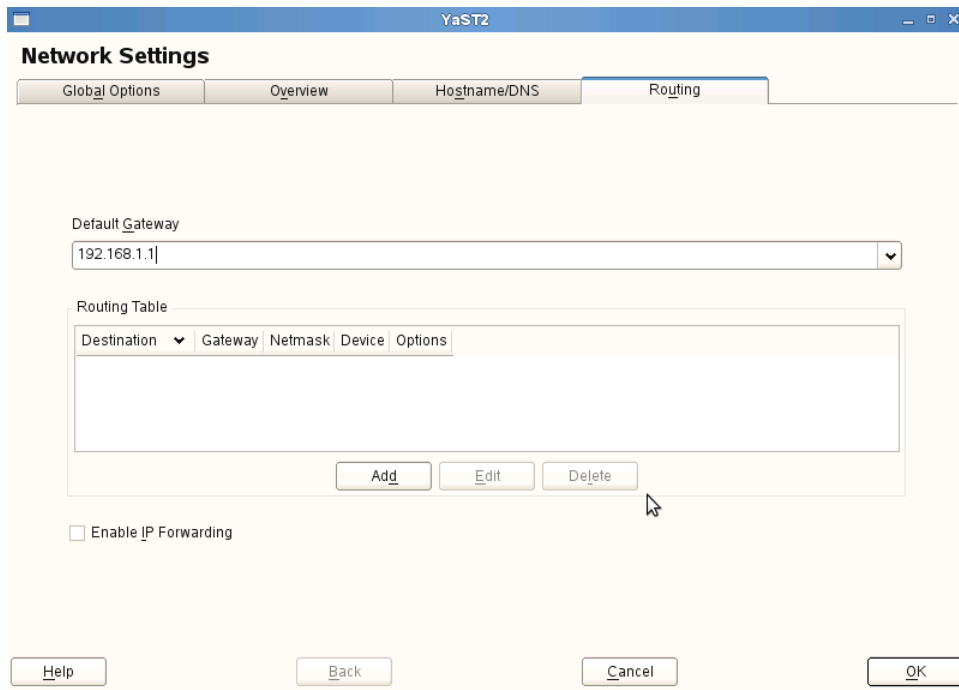
- Setelah konfigurasi squid sudah selesai, jalankan service squid proxy dengan perintah # **rcsquid start** dan jalankan perintah # **inserv squid** sehingga service squid berjalan otomatis pada saat booting server

setelah konfigurasi squid selesai, kita harus melakukan beberapa routing di server tersebut karena memiliki 2 buah NIC, routing ini di maksudkan untuk otomatis meredirect port 80 ke port 3128 (proxy transparent) sehingga tidak perlu konfigurasi manual pada web browser pc klien. NIC yang pertama akan terhubung dengan modem, kemudian NIC yang kedua akan menjadi gateway untuk setiap klien PC.

MODEM ===== NIC1 Server NIC 2 ===== Switch === PC Client



- Lakukan konfigurasi NIC, dengan menjalankan perintah # **yast2 lan** lalu setting ip address eth0 dan eth1 seperti contoh gambar di atas



- lalu setting dengan ip gateway yaitu ip modem, contoh 192.168.1.1 adalah ip modem lalu klik OK untuk menyelesaikan konfigurasi

```
File Edit View Scrollback Bookmarks Settings Help
### /etc/resolv.conf file autogenerated by netconfig!
#
# Before you change this file manually, consider to define the
# static DNS configuration using the following variables in the
# /etc/sysconfig/network/config file:
#   NETCONFIG_DNS_STATIC_SEARCHLIST
#   NETCONFIG_DNS_STATIC_SERVERS
#   NETCONFIG_DNS_FORWARDER
# or disable DNS configuration updates via netconfig by setting:
#   NETCONFIG_DNS_POLICY=''
#
# See also the netconfig(8) manual page and other documentation.
#
# Note: Manual change of this file disables netconfig too, but
# may get lost when this file contains comments or empty lines
# only, the netconfig settings are same with settings in this
# file and in case of a "netconfig update -f" call.
#
### Please remove (at least) this line when you modify the file!
nameserver 202.134.0.155
nameserver 202.134.2.5
-- REPLACE --
21, 23 All
dimaz : vi
```

- setelah itu konfigurasi ip dns dengan mengedit file /etc/resolv.conf lalu isikan ip dns speedy, contoh 202.134.0.155, 202.134.2.5 lalu save file tersebut

setelah konfigurasi squid, ip address dan dns sudah dilakukan, langkah terakhir yaitu melakukan routing sehingga paket-paket dari pc client akan melewati squid proxy.

- Ketikkan perintah dibawah (pada saat menentukan eth0 dan eth1 pada perintah dibawah tidak terbalik ! Konfigurasi ini eth0 menghadap ke modem dan eth1 menghadap ke client)

```
# iptables --append FORWARD -i eth1 -j ACCEPT
# iptables -A PREROUTING -t nat -j REDIRECT -p tcp -i eth1 --dport 80 --to-ports 3128
# iptables -t nat --append POSTROUTING -o eth0 -j MASQUERADE
# iptables-save
# echo 1 > /proc/sys/net/ipv4/ip_forward
```

kemudian edit file **/etc/init.d/boot.local** lalu ketikkan ulang sintaks-sintaks diatas, sehingga pada saat server boot, otomatis sintaks diatas akan dijalankan juga.