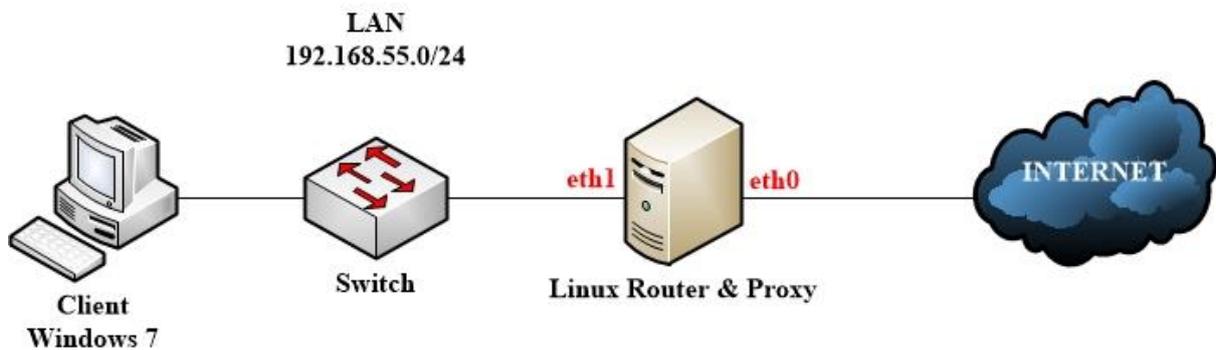


## Membangun PC Router dan Proxy Server pada Linux CentOS

Oleh I Putu Hariyadi

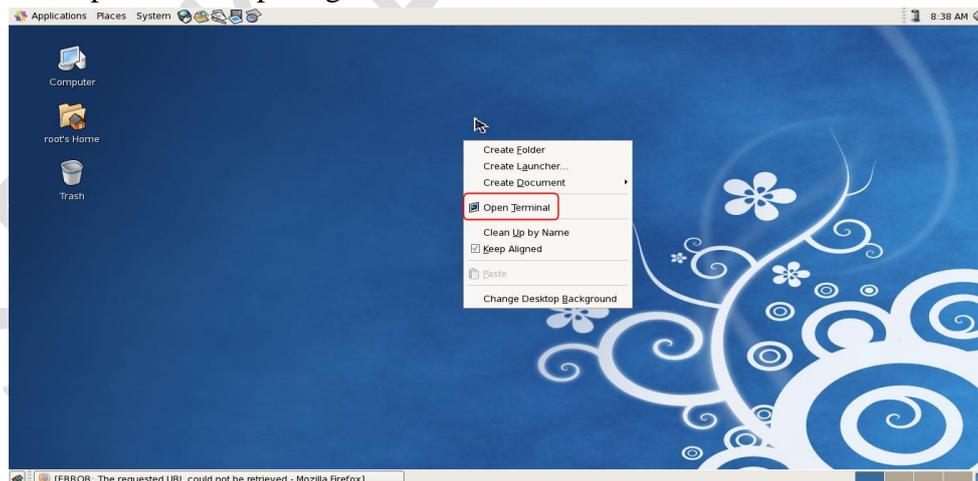
< [putu.hariyadi@stmikbumigora.ac.id](mailto:putu.hariyadi@stmikbumigora.ac.id) >



### KONFIGURASI KOMPUTER SERVER LINUX CENTOS

#### A. Mengatur Pengalamatan IP pada interface jaringan dan mengaktifkan fitur forwarding

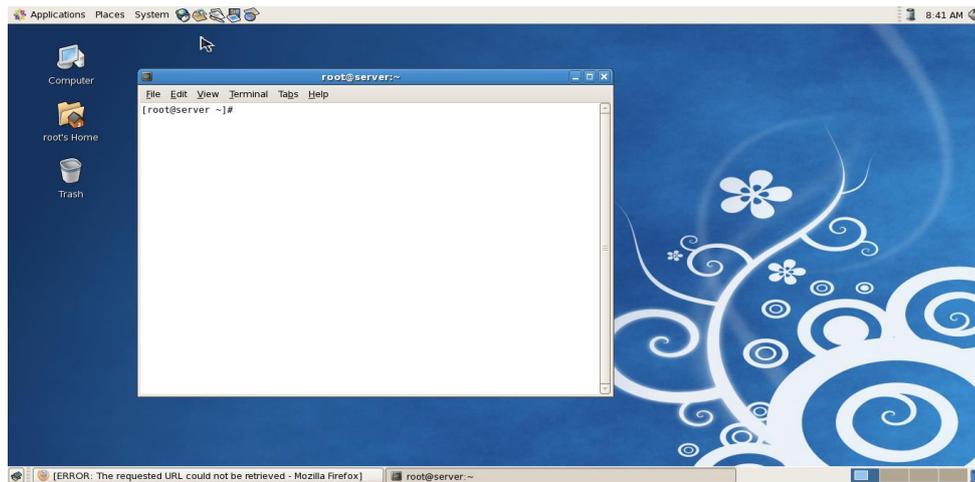
1. Login ke Linux menggunakan user “**root**” dengan sandi login “**123456**”.
2. Buka terminal Linux dengan cara klik kanan pada desktop kemudian pilih **Open Terminal**, seperti terlihat pada gambar berikut:



Selanjutnya akan tampil kotak dialog terminal seperti terlihat pada gambar berikut:

## Modul Pengabdian untuk SMKN 1 Labuapi Lombok Barat

---



3. Berpindah ke lokasi direktori yg memuat file konfigurasi interface jaringan

```
# cd /etc/sysconfig/network-scripts
```

4. Menampilkan informasi di direktori mana saat ini berada menggunakan perintah:

```
# pwd
```

5. Melihat isi direktori dimana saat ini berada menggunakan perintah:

```
# ls
```

6. Mengatur pengalamatan IP untuk interface jaringan eth0 yang terhubung ke Internet

- a. Buka file konfigurasi *ifcfg-eth0* menggunakan editor nano

```
# nano ifcfg-eth0
```

DEVICE=eth0 ← nama pengenal perangkat interface jaringan oleh Linux

BOOTPROTO=none ← metode alokasi IP yg digunakan, “none” untuk alokasi secara statik

NETWORK=172.16.17.128 ← mengatur alamat jaringan (**sesuaikan ketika ujian**)

IPADDR=172.16.17.130 ← mengatur alamat IP (**sesuaikan ketika ujian**)

NETMASK=255.255.255.192 ← mengatur alamat subnetmask (**sesuaikan ketika ujian**)

GATEWAY=172.16.17.129 ← mengatur alamat gateway (**sesuaikan ketika ujian**)

ONBOOT=yes ← mengatur agar interface langsung diaktifkan ketika booting pertama kali

HWADDR= ← Alamat MAC Address (**JANGAN DIUBAH**)

- b. Menyimpan perubahan konfigurasi tekan **CTRL+O > Enter**

- c. Keluar dari editor nano tekan **CTRL+X**

## Modul Pengabdian untuk SMKN 1 Labuapi Lombok Barat

7. Mengatur pengalamanan IP untuk interface jaringan *eth1* yang terhubung ke LAN

a. Buka file konfigurasi *ifcfg-eth1* menggunakan editor nano

```
# nano ifcfg-eth1
```

DEVICE=eth1 ← nama pengenalan perangkat interface jaringan oleh Linux

BOOTPROTO=none ← metode alokasi IP yg digunakan, “none” untuk alokasi secara statik

NETWORK=192.168.55.0 ← mengatur alamat jaringan (**sesuaikan ketika ujian**)

IPADDR=192.168.55.1 ← mengatur alamat IP (**sesuaikan ketika ujian**)

NETMASK=255.255.255.0 ← mengatur alamat subnetmask (**sesuaikan ketika ujian**)

ONBOOT=yes ← mengatur agar interface langsung diaktifkan ketika booting pertama kali

HWADDR= ← Alamat MAC Address (**JANGAN DIUBAH**)

b. Menyimpan perubahan konfigurasi tekan **CTRL+O > Enter**

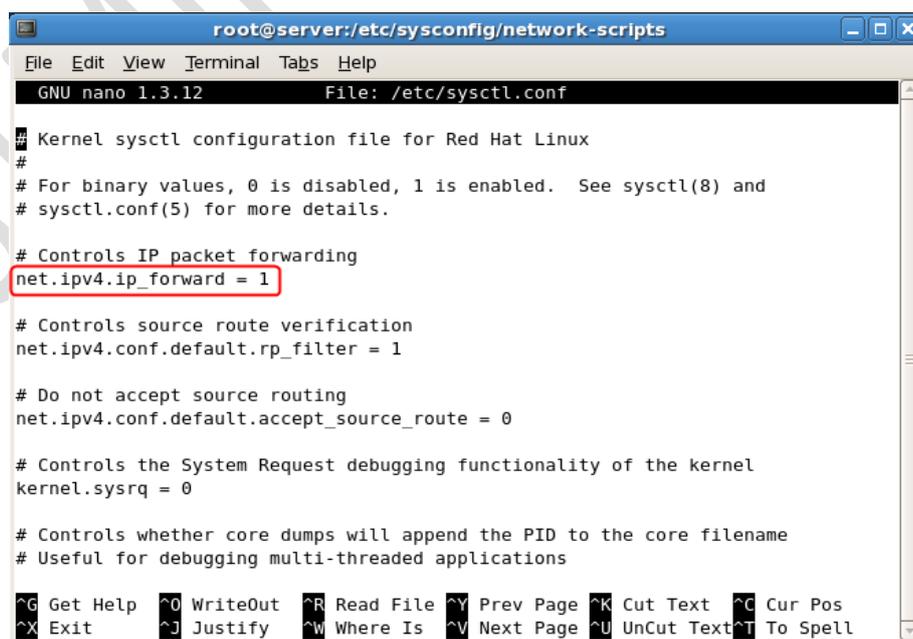
c. Keluar dari editor nano tekan **CTRL+X**

8. Mengaktifkan fitur forwarding agar mendukung routing di file */etc/sysctl.conf*

a. Buka file konfigurasi *sysctl.conf* menggunakan editor nano

```
# nano /etc/sysctl.conf
```

Ubah nilai dari parameter `net.ipv4.ip_forward` dari nilai awal **0** yang bermakna *disable* (dinonaktifkan) menjadi **1** yang bermakna *enable* (diaktifkan), seperti terlihat pada gambar berikut:



```
root@server:/etc/sysconfig/network-scripts
File Edit View Terminal Tabs Help
GNU nano 1.3.12 File: /etc/sysctl.conf
# Kernel sysctl configuration file for Red Hat Linux
#
# For binary values, 0 is disabled, 1 is enabled. See sysctl(8) and
# sysctl.conf(5) for more details.
# Controls IP packet forwarding
net.ipv4.ip_forward = 1
# Controls source route verification
net.ipv4.conf.default.rp_filter = 1
# Do not accept source routing
net.ipv4.conf.default.accept_source_route = 0
# Controls the System Request debugging functionality of the kernel
kernel.sysrq = 0
# Controls whether core dumps will append the PID to the core filename
# Useful for debugging multi-threaded applications
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell
```

## Modul Pengabdian untuk SMKN 1 Labuapi Lombok Barat

---

- b. Menyimpan perubahan konfigurasi tekan **CTRL+O > Enter**
  - c. Keluar dari editor nano tekan **CTRL+X**
9. Merestart *service network* untuk mengaktifkan perubahan pengalamatan IP pada interface *eth0* dan *eth1*, serta fitur *forwarding*

```
# service network restart
```

10. Menampilkan informasi pengalamatan IP yang digunakan oleh interface

```
# ifconfig
```

11. Menguji apakah protokol TCP/IP telah terinstall dengan baik atau belum

```
# ping localhost
```

Untuk menghentikan *ping* gunakan **CTRL+C**

12. Menguji interface jaringan *eth0* dan *eth1* telah berfungsi telah baik atau belum

```
# ping 172.16.17.130 ← sesuaikan alamat IP ini ketika ujian
```

```
# ping 192.168.55.1 ← sesuaikan alamat IP ini ketika ujian
```

13. Menampilkan informasi table routing

```
# route -n
```

### B. Mengatur DNS Client untuk proses resolusi nama domain

1. Buka file konfigurasi */etc/resolv.conf* menggunakan editor nano

```
# nano /etc/resolv.conf
```

```
nameserver 202.152.5.36 ← sesuaikan alamat IP DNS ini ketika ujian
```

```
nameserver 8.8.8.8 ← sesuaikan alamat IP DNS ini ketika ujian
```

```
nameserver 8.8.4.4 ← sesuaikan alamat IP DNS ini ketika ujian
```

2. Menyimpan perubahan konfigurasi tekan **CTRL-O > Enter**
3. Keluar dari editor nano tekan **CTRL-X**

### C. Mengatur Internet Connection Sharing (ICS) dan Transparent Proxy menggunakan IPTables

1. Membersihkan aturan IPTables di table *filter*, *nat*, dan *mangle*

## Modul Pengabdian untuk SMKN 1 Labuapi Lombok Barat

---

```
# iptables -F
# iptables -t nat -F
# iptables -t mangle -F
```

2. Mengatur ICS agar dapat berbagi pakai koneksi Internet ke client

```
# iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

3. Mengatur transparent proxy

```
# iptables -t nat -A PREROUTING -i eth1 -p tcp -m tcp
--dport 80 -j REDIRECT --to-ports 3128
```

**Perhatian: perintah iptables ini ditulis dalam 1 baris**

4. Menyimpan konfigurasi IPTables secara permanen

```
# service iptables save
```

5. Mengaktifkan *service iptables*

```
# service iptables start
```

6. Memverifikasi hasil konfigurasi IPTables

```
# service iptables status
```

Hasil dari eksekusi perintah tersebut, seperti terlihat pada gambar berikut:

```
Table: nat
Chain PREROUTING (policy ACCEPT)
num target prot opt source destination
1 REDIRECT tcp -- 0.0.0.0/0 0.0.0.0/0 tcp dpt:80 redir ports 3128

Chain POSTROUTING (policy ACCEPT)
num target prot opt source destination
1 MASQUERADE all -- 0.0.0.0/0 0.0.0.0/0

Chain OUTPUT (policy ACCEPT)
num target prot opt source destination

Table: filter
Chain INPUT (policy ACCEPT)
num target prot opt source destination

Chain FORWARD (policy ACCEPT)
num target prot opt source destination

Chain OUTPUT (policy ACCEPT)
num target prot opt source destination
```

### D. Menginstalasi paket aplikasi Squid untuk proxy server

1. Mengakses DVD-ROM (Secara default telah termount oleh Linuxnya). Berpindah ke lokasi direktori mount dari DVD-ROM

```
# cd /media/CentOS_5.6_Final/CentOS
```

atau cara cepat

```
# cd /media/C<tekan-tab>/C<tekan-tab>
```

2. Menampilkan informasi di direktori mana saat ini berada menggunakan perintah:

```
# pwd
```

3. Menginstalasi paket aplikasi perl-URI dan squid

```
#rpm -ivh perl-URI-1.35-3.noarch.rpm squid-2.6.STABLE21-6.el5.i386.rpm
```

atau cara cepat

```
#rpm -ivh perl-URI<TEKAN TAB> squid<TEKAN TAB>
```

4. Memverifikasi apakah paket aplikasi squid telah terinstalasi atau belum

```
#rpm -q squid
```

### E. Mengatur konfigurasi file squid.conf

1. Berpindah direktori ke lokasi yang memuat file konfigurasi utama *squid* yaitu di direktori */etc/squid*

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

2. Menampilkan informasi di direktori mana saat ini berada menggunakan perintah:

```
# pwd
```

3. Melihat isi dari direktori saat ini berada menggunakan perintah

```
# ls
```

4. Membuat salinan file *squid.conf* dengan nama *squid.conf.backup* menggunakan perintah:

```
# cp squid.conf squid.conf.backup
```

5. Melihat isi dari direktori saat ini berada untuk memastikan file salinan yang telah berhasil dibuat menggunakan perintah

```
# ls
```

6. Mengubah file konfigurasi *squid.conf*

- a. Buka file konfigurasi *squid.conf* menggunakan editor nano

```
# nano squid.conf
```

Untuk mempermudah konfigurasi *directive* dari squid, maka akan digunakan fitur pencarian dari editor **nano** dengan menekan **CTRL+W**.

## Modul Pengabdian untuk SMKN 1 Labuapi Lombok Barat

---

Tekan **CTRL+W**, masukan kata kunci pencarian “**http\_port 3128**” dan tekan **Enter**. Tampil baris dengan nilai sesuai dengan kata kunci pencarian yang digunakan, terlihat seperti berikut:

```
http_port 3128
```

Directive **http\_port** berfungsi untuk menentukan nomor port yang digunakan proxy server, secara default telah menggunakan nomor **3128**. Selanjutnya tambahkan parameter “**transparent**” dibelakang directive **http\_port 3128** agar proxy server mendukung fitur *transparent proxy*, sehingga terlihat seperti berikut:

```
http_port 3128 transparent
```

Tambahkan konfigurasi *directive* squid lainnya dibawah baris **http\_port 3128 transparent** ditulis satu *directive* per baris, yaitu antara lain:

```
cache_mgr iputu.hariyadi@smkn1labuapi.sch.id
```

```
visible_hostname www.smkn1labuapi.sch.id
```

```
cache_mem 64 MB
```

```
cache_swap_low 90
```

```
cache_swap_high 95
```

```
ipcache_size 1024
```

```
ipcache_low 90
```

```
ipcache_high 95
```

```
cache_dir ufs /var/spool/squid 100 16 256
```

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

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

```
dns_nameservers 202.152.5.36 8.8.8.8 8.8.4.4
```

## Modul Pengabdian untuk SMKN 1 Labuapi Lombok Barat

Tekan **CTRL+W**, masukan kata kunci pencarian “**# INSERT**” dan tekan **Enter**. Tampil baris dengan nilai sesuai dengan kata kunci pencarian yang digunakan, terlihat seperti pada gambar yang ditandai dengan kotak berwarna merah berikut:

```
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS

# Example rule allowing access from your local networks. Adapt
# to list your (internal) IP networks from where browsing should
# be allowed
#acl our_networks src 192.168.1.0/24 192.168.2.0/24
#http_access allow our_networks

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

Lanjutkan penambahan konfigurasi *directive* squid lainnya yaitu terkait *Access Control List (ACL)* dan pengaturan aksesnya dibawah baris “**# INSERT YOUR OWN RULE(S) ...**”, yaitu:

```
acl domain_terlarang dstdomain "/etc/squid/domain_terlarang"
http_access deny domain_terlarang

acl ip_terlarang dst "/etc/squid/ip_terlarang"
http_access deny ip_terlarang

acl kata_terlarang url_regex -i "/etc/squid/kata_terlarang"
http_access deny kata_terlarang

acl SMK src 192.168.55.0/24
http_access allow SMK
```

- Menyimpan perubahan konfigurasi tekan **CTRL+O > Enter**
- Keluar dari editor nano tekan **CTRL+X**
- Penjelasan dari masing-masing *directive* yang dikonfigurasi pada file *squid.conf* terdapat pada tabel berikut:

Directive	Deskripsi
http_port 3128 transparent	Menentukan nomor port yang digunakan oleh squid dan

## Modul Pengabdian untuk SMKN 1 Labuapi Lombok Barat

	mengaktifkan dukungan transparent proxy
cache_mgr <a href="mailto:iputu_hariyadi@smkn1labuapi.sch.id">iputu_hariyadi@smkn1labuapi.sch.id</a>	Menentukan alamat e-mail dari local cache manager yang akan menerima pesan apabila cache mati.
visible_hostname www.smkn1labuapi.sch.id	Menentukan nama host yang akan ditampilkan oleh cache pada pesan kesalahan yang tampil.
cache_mem 64 MB	Menentukan besar memory yang digunakan oleh squid cache
cache_swap_low 90 cache_swap_high 95	Menentukan squid akan mulai menghapus object yang tersimpan di hardisk bila batas (swap_low) atas telah tercapai, dan jika batas atas sekali tercapai (swap_high) squid semakin sering menghapus sampai pada batas atas terpenuhi.
ipcache_size 1024	Menentukan ukuran dari <i>ip cache</i> yang digunakan oleh squid cache
ipcache_low 90 ipcache_high 95	Menentukan squid akan mulai menghapus cache IP yang tersimpan bila batas (cache_low) atas telah tercapai, dan jika batas atas sekali tercapai (cache_high) squid semakin sering menghapus sampai pada batas atas terpenuhi.
cache_dir ufs /var/spool/squid 100 16 256	Menentukan jenis system penyimpanan yang digunakan, lokasi direktori penyimpanan cache, ukuran cache, dan jumlah direktori yang terdapat di dalam direktori cache.
cache_log /var/log/squid/cache.log	Menentukan lokasi file penyimpanan log aktivitas cache.
cache_store_log /var/log/squid/store.log	Menentukan lokasi file penyimpanan log aktivitas yang dilakukan oleh storage manager.
dns_nameservers 202.152.5.36 8.8.8.8 8.8.4.4	Menentukan alamat IP dari server DNS
acl domain_terlarang dstdomain "/etc/squid/domain_terlarang"	Membuat access control list dengan nama <b>domain_terlarang</b> untuk mengatur ijin akses berdasarkan nama domain dari situs yang diakses. Nama domain yang diatur ijin aksesnya disimpan pada sebuah file dengan lokasi di

## Modul Pengabdian untuk SMKN 1 Labuapi Lombok Barat

	<b>/etc/squid/domain_terlarang</b>
<code>http_access deny domain_terlarang</code>	Menolak akses untuk ACL dengan nama <b>domain_terlarang</b>
<code>acl ip_terlarang dst "/etc/squid/ip_terlarang"</code>	Membuat access control list dengan nama <b>ip_terlarang</b> untuk mengatur ijin akses berdasarkan alamat IP dari situs yang diakses. Alamat IP yang diatur ijin aksesnya disimpan pada sebuah file dengan lokasi di <b>/etc/squid/ip_terlarang</b>
<code>http_access deny ip_terlarang</code>	Menolak akses untuk ACL dengan nama <b>ip_terlarang</b>
<code>acl kata_terlarang url_regex -i "/etc/squid/kata_terlarang"</code>	Membuat access control list dengan nama <b>kata_terlarang</b> untuk mengatur ijin akses berdasarkan kata yang terkandung pada URL dari situs yang diakses. Kata-kata yang diatur ijin aksesnya disimpan pada sebuah file dengan lokasi di <b>/etc/squid/kata_terlarang</b>
<code>http_access deny kata_terlarang</code>	Menolak akses untuk ACL dengan nama <b>kata_terlarang</b>
<code>acl SMK src 192.168.55.0/24</code>	Membuat <i>access control list</i> dengan nama <b>SMK</b> untuk mengatur ijin akses berdasarkan alamat sumber jaringan 192.168.55.0/24
<code>http_access allow SMK</code>	Mengijinkan akses untuk ACL dengan nama <b>SMK</b>

7. Membuat file yang memuat daftar situs yang diblokir berdasarkan nama domain
  - a. Buat file dengan nama "**domain\_terlarang**" menggunakan editor **nano**  
# nano domain\_terlarang
  - b. Masukkan nama domain yang diblokir, sebagai contoh **www.google.com** dan **www.yahoo.com**. Ketentuan penulisan adalah satu baris memuat satu nama domain.
  - c. Menyimpan perubahan tekan **CTRL+O > Enter**
  - d. Keluar dari editor nano tekan **CTRL+X**
  
8. Membuat file yang memuat daftar situs yang diblokir berdasarkan alamat IP
  - a. Buat file dengan nama "**ip\_terlarang**" menggunakan editor **nano**  
# nano ip\_terlarang
  
  - b. Masukkan alamat IP yang diblokir, sebagai contoh **203.190.241.43** yang merupakan alamat IP dari situs **detik.com**. Ketentuan penulisan adalah satu baris memuat satu alamat IP.

## Modul Pengabdian untuk SMKN 1 Labuapi Lombok Barat

---

- c. Menyimpan perubahan tekan **CTRL+O > Enter**
  - d. Keluar dari editor nano tekan **CTRL+X**
9. Membuat file yang memuat daftar situs yang diblokir berdasarkan kata yang terdapat pada URL
- a. Buat file dengan nama “**kata\_terlarang**” menggunakan editor **nano**  

```
# nano kata_terlarang
```
  - b. Masukkan kata yang diblokir, sebagai contoh **facebook**. Ketentuan penulisan adalah satu baris memuat satu kata.
  - c. Menyimpan perubahan tekan **CTRL+O > Enter**
  - d. Keluar dari editor nano tekan **CTRL+X**
10. Mengaktifkan service squid

```
# service squid start
```

Apabila muncul pesan kesalahan ketika mengeksekusi perintah diatas maka untuk mempermudah dan mempercepat mengetahui lokasi penyebab kesalahan tersebut dapat melihat isi file “**squid.out**” yang terdapat di direktori **/var/log/squid** menggunakan perintah berikut:

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

11. Memverifikasi status service squid telah berjalan atau belum

```
#service squid status
```

Catatan:

Apabila Anda melakukan perubahan kembali pada file konfigurasi “**squid.conf**”, maka Anda perlu mengeksekusi perintah berikut agar perubahan tersebut diaktifkan

```
# service squid reload
```

### KONFIGURASI KOMPUTER CLIENT WINDOWS 7

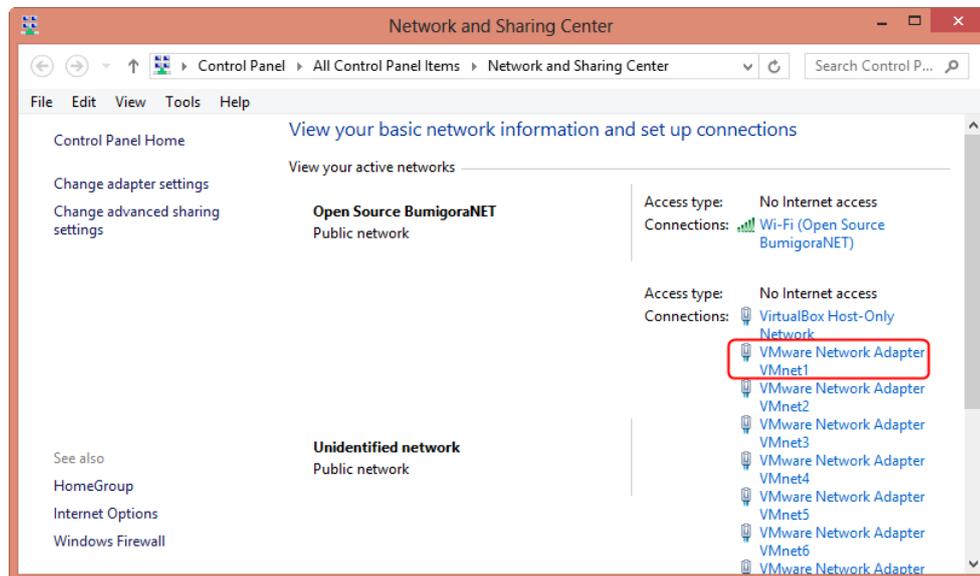
Adapun langkah-langkah konfigurasi yang dilakukan pada computer client Windows 7 adalah sebagai berikut:

1. Mengatur pengalamatan IP dan parameter TCP/IP lainnya melalui **taskbar bagian pojok kanan bawah** dengan cara **klik kanan** pada icon **Network** dan pilih **Open Network & Sharing Center**, seperti terlihat pada gambar berikut:

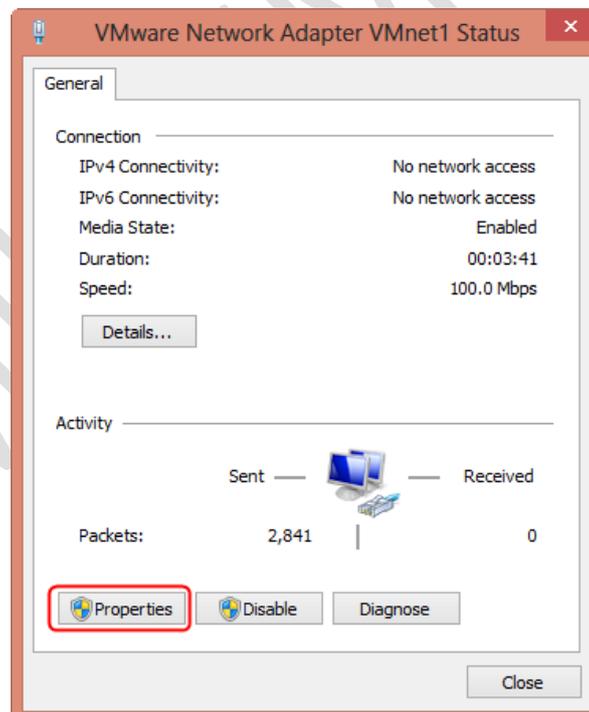


## Modul Pengabdian untuk SMKN 1 Labuapi Lombok Barat

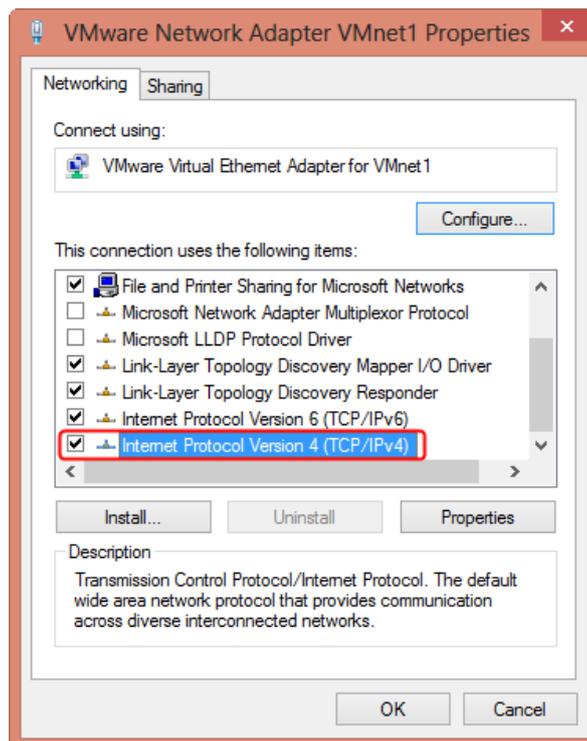
2. Tampil kotak dialog **Network and Sharing Center**. Klik pada adapter **VirtualBox Host-Only Network**, seperti terlihat pada gambar berikut:



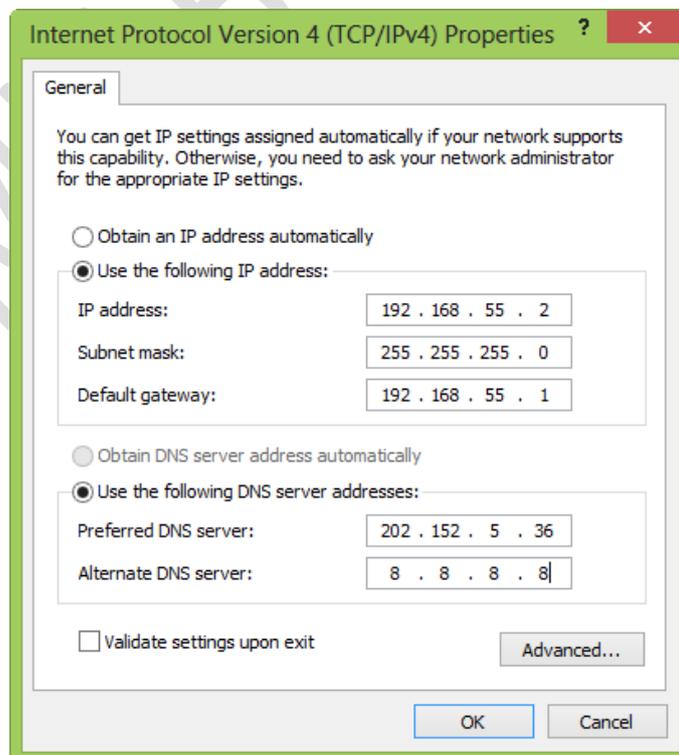
3. Tampil kotak dialog **VMware Network Adapter VMNet1 Status**. Klik tombol **Properties**, seperti terlihat pada gambar berikut:



4. Tampil kotak dialog **VMware Network Adapter VMNet1 Properties**. Pada bagian **“This connection uses the following items:”**, klik dua kali pada pilihan **Internet Protocol Version 4 (TCP/IPv4)**, seperti terlihat pada gambar berikut:



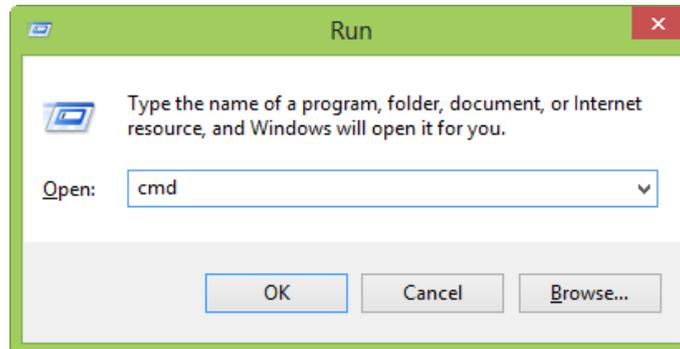
5. Tampil kotak dialog **Internet Protocol Version 4 (TCP/IPv4) Properties**. Pilih Use the following IP Address untuk mengalokasikan alamat IP dan pengaturan parameter TCP/IP lainnya secara manual Lengkapi parameter *IP Address*, *Subnetmask*, *Default Gateway*, *Preffered DNS Server*, dan *Alternate DNS Server*, seperti terlihat pada gambar berikut:



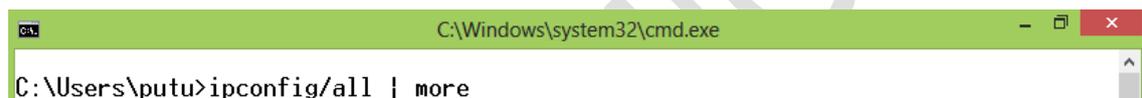
## Modul Pengabdian untuk SMKN 1 Labuapi Lombok Barat

Klik tombol **OK > OK > OK > Close**. Tutup kotak dialog **Network and Sharing Center**.

6. Buka **Command Prompt Windows** dengan menekan tombol **Windows+R**. Pada inputan form yang tampil, ketik "**cmd**" dan tekan tombol **Enter**.



7. Pada **Command Prompt** masukkan perintah "**ipconfig/all | more**" untuk memverifikasi pengalamatan IP yang telah diatur, seperti terlihat pada gambar berikut:



Pastikan pengalamatan IP yang digunakan oleh adapter **VMware Network Adapter VMnet1** seperti yang telah ditentukan sebelumnya, seperti terlihat pada gambar berikut:

Ethernet adapter VMware Network Adapter VMnet1:

```
Connection-specific DNS Suffix . . . : 
Description . . . . . : VMware Virtual Ethernet Adapter for VMnet
1 Physical Address. . . . . : 00-50-56-C0-00-01
  DHCP Enabled. . . . . : No
  Autoconfiguration Enabled . . . . : Yes
  Link-local IPv6 Address . . . . . : fe80::c88c:790e:cfd6:d668%20(Preferred)
  IPv4 Address. . . . . : 192.168.55.2(Preferred)
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.55.1
  DHCPv6 IAID . . . . . : 637554774
  DHCPv6 Client DUID. . . . . : 00-01-00-01-19-F0-EF-78-20-6A-8A-EF-D3-EA
  DNS Servers . . . . . : 202.152.5.36
                           8.8.8.8
  NetBIOS over Tcpi. . . . . : Enabled
```

Tekan tombol **spasi** untuk menampilkan layar berikutnya. Tekan tombol **q** untuk keluar.

8. Verifikasi koneksi dari *client Windows 7* ke *interface eth1* dari *Server Linux* menggunakan perintah "**ping 192.168.55.1**" pada **Command Prompt Windows**, seperti terlihat pada gambar berikut:

## Modul Pengabdian untuk SMKN 1 Labuapi Lombok Barat

```
C:\Windows\system32\cmd.exe

C:\Users\putu>ping 192.168.55.1

Pinging 192.168.55.1 with 32 bytes of data:
Reply from 192.168.55.1: bytes=32 time<1ms TTL=64

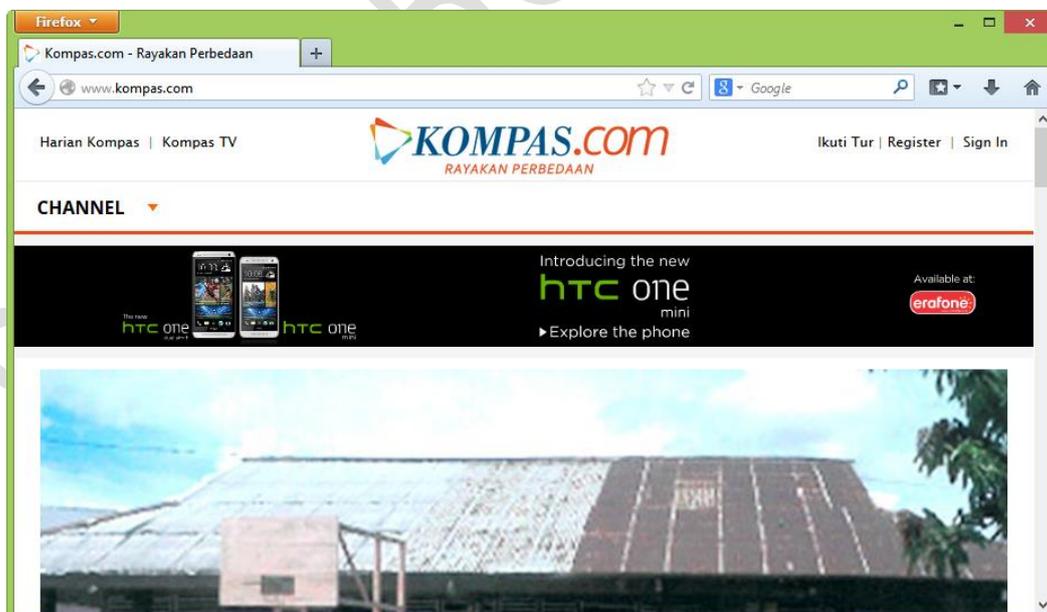
Ping statistics for 192.168.55.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

9. Verifikasi koneksi ke alamat gateway ISP yang digunakan menggunakan perintah “**ping 172.16.17.129**” pada **Command Prompt Windows**, yaitu

C:\Users\putu> **ping 172.16.17.129** ← disesuaikan ketika ujian

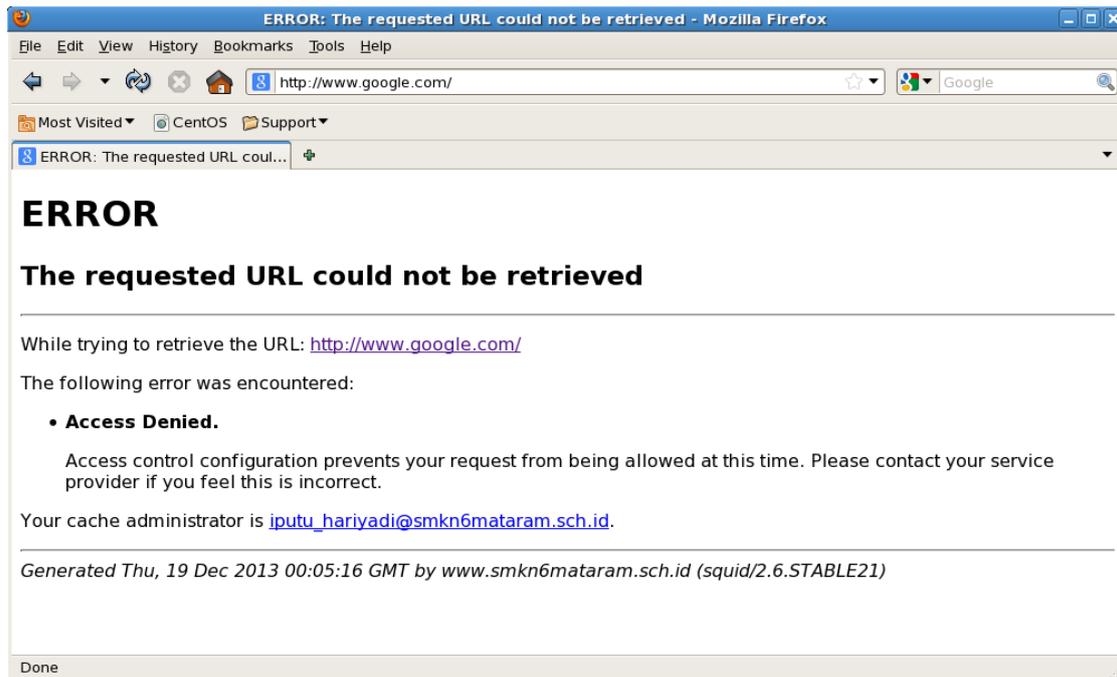
### UJICOBA KONEKSI INTERNET DARI CLIENT WINDOWS 7

1. Buka browser **Mozilla Firefox** melalui menu **Start → All Programs → Mozilla Firefox**. Atau dengan mengakses icon Firefox yang terdapat pada taskbar.
2. Pada address bar dari browser **Firefox**, masukkan alamat situs yang diijinkan untuk diakses, sebagai contoh <http://www.kompas.com>. Hasil ujicoba seperti terlihat pada gambar berikut:

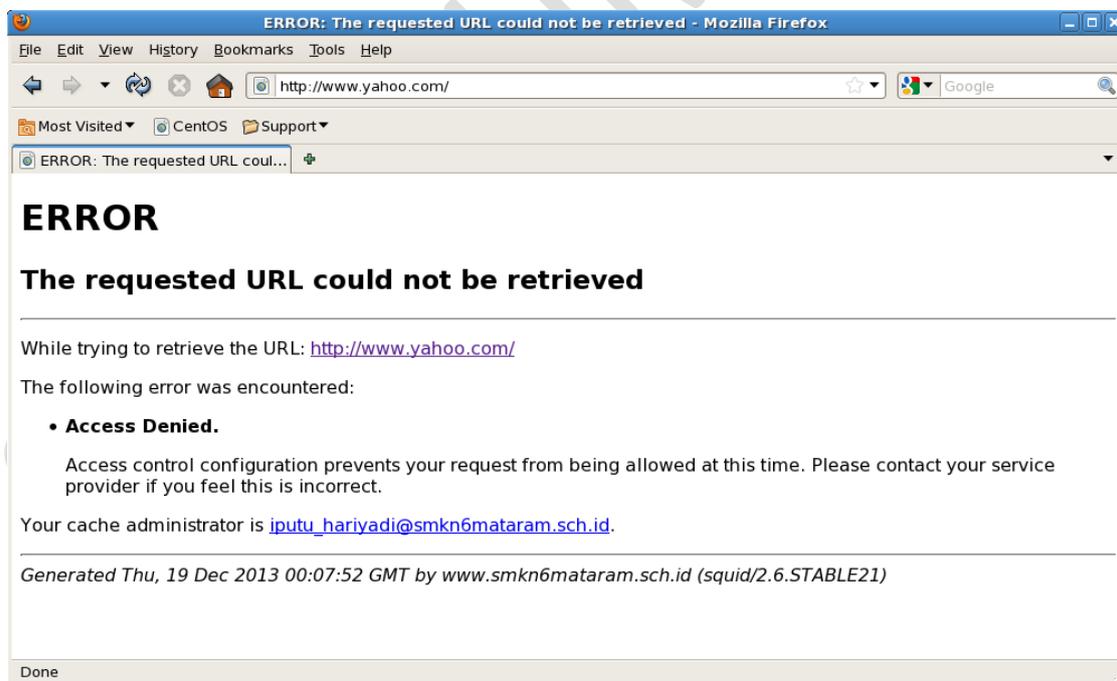


3. Lakukan ujicoba dengan mengakses situs yang telah diatur untuk diblokir pada proxy server berdasarkan nama domain, sebagai contoh untuk domain [www.google.com](http://www.google.com). Hasil ujicoba seperti terlihat pada gambar berikut:

# Modul Pengabdian untuk SMKN 1 Labuapi Lombok Barat

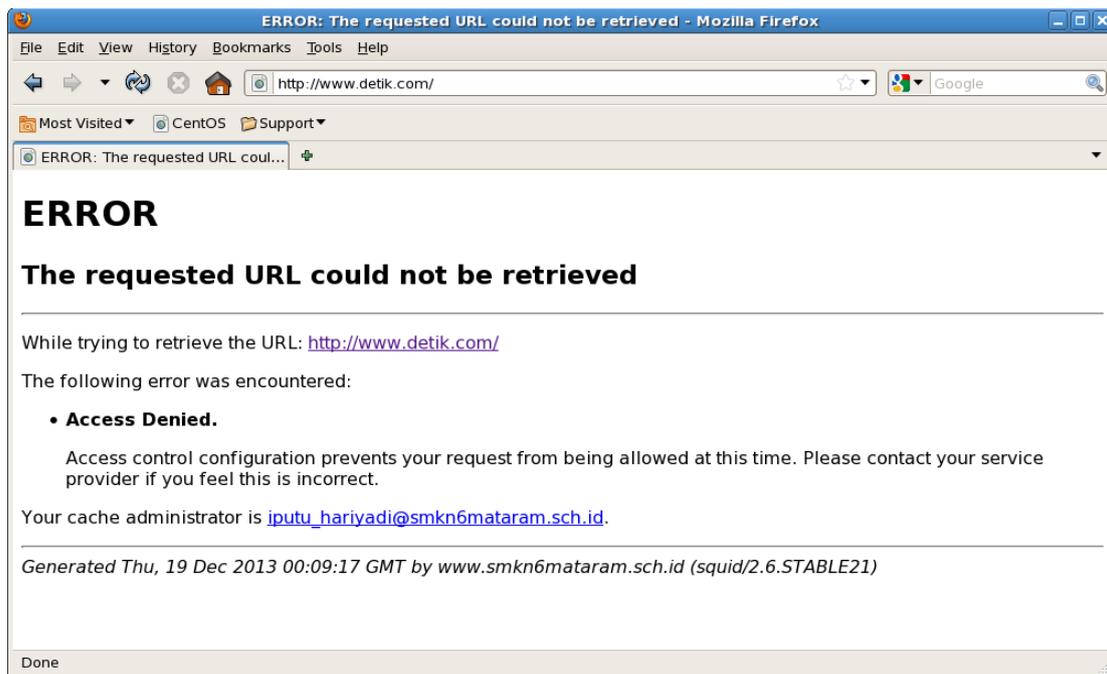


4. Lakukan ujicoba dengan mengakses situs yang telah diblokir berdasarkan nama domain, lainnya sebagai contoh untuk domain [www.yahoo.com](http://www.yahoo.com). Hasil ujicoba seperti terlihat pada gambar berikut:

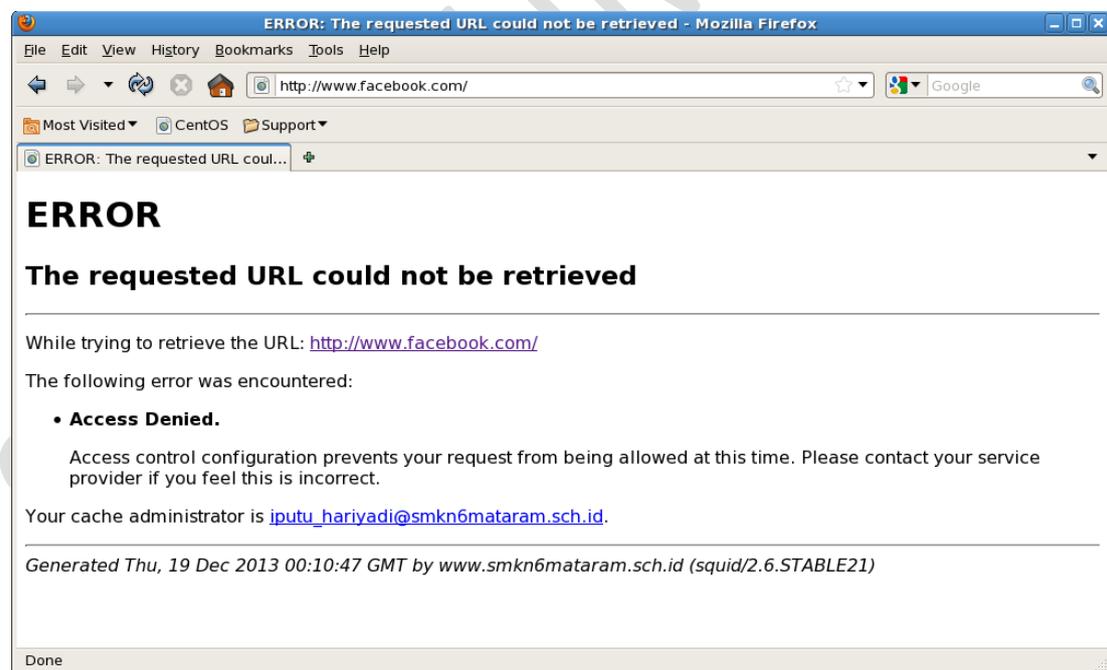


5. Lakukan ujicoba dengan mengakses situs yang telah diblokir berdasarkan alamat IP, sebagai contoh "203.190.241.43" yang merupakan alamat IP dari situs "detik.com". Hasil ujicoba seperti terlihat pada gambar berikut:

## Modul Pengabdian untuk SMKN 1 Labuapi Lombok Barat



6. Lakukan ujicoba dengan mengakses situs yang telah diblokir berdasarkan kata yang terdapat pada **URL**, sebagai contoh yang mengandung kata “facebook”. Hasil ujicoba seperti terlihat pada gambar berikut:



**Selamat Anda telah sukses membangun PC Router dan Proxy Server menggunakan Linux CentOS ☺**