

# Modul Membangun Proxy Server untuk Warnet & RTRW Net di Ubuntu 14.04 Server (Day 2)

## Konfigurasi Squid Proxy

Backup terlebih dahulu file konfigurasi squid.conf yang default :

```
# mv /etc/squid/squid.conf /etc/squid/squid.conf.backup
```

Setelah itu download file konfigurasi squid.conf yang baru, ekstrak, dan juga pindahkan konfigurasinya ke folder /etc/squid :

```
# wget http://cilsy.id/upload/squid.conf.tar.gz
# tar -xvf squid.conf.tar.gz
# mv squid.conf /etc/squid/
# mv store-id.pl /etc/squid/
```

Ada 2 file konfigurasi utama squid ini. Yaitu squid.conf dan store-id.pl. Pada dasarnya kedua file konfig ini sudah bisa langsung berjalan jika kalian mengikuti topologi maupun ip-ip yang sama dari seluruh rangkaian tutorial ini. Tapi kalau ada yang perlu disesuaikan, kalian bisa coba buka file konfigurasi squid.conf :

```
# nano /etc/squid/squid.conf
```

Kita akan melakukan beberapa konfigurasi dan penyesuaian sebagai berikut :

### Menentukan Jaringan lokal

Cari baris :

```
acl localnet src 192.168.30.0/24
```

Sesuaikan dengan jaringan lokal kalian.

### Menentukan Direktori Cache dan cara menghitungnya

Cari baris :

```
cache_dir aufs /proxy 16000 37 256
```

Untuk yang saya warnai oren, itu adalah letak folder partisi cache kalian. Untuk yang biru, angka 16000 adalah ukuran partisi dalam MB. Jadi 16000 adalah 16GB. Nah disini kalian gunakan dalam satuan KB. jadi 16GB = 16.000.000. Untuk yang warna merah, itu sudah standar 256 biarkan saja. Sedangkan untuk yang warna hijau cara menghitungnya begini :

$$(((x / y) / 256) / 256) * 2 = \text{warna hijau}$$

x = besarnya disk cache yang akan di gunakan, satuannya adalah Kb (16 GB = 16.000.000 KB)  
y = jumlah rata-rata object biasanya bernilai 13Kb

Misalkan besarnya cache disk yang akan kita pakai adalah 16 GB maka:

$$(((16.000.000/13)/256)/256)*2 = 37$$

Maka nilai yang warna hijau adalah 37.

Maka baris konfigurasi kalian benar nilainya :

```
cache_dir ufs /proxy 16000 37 256
```

16GB didapat dari 80% x nilai total partisi cache. Ini adalah nilai optimalnya.

Jika sudah simpan file dengan menekan CTRL + X > Y > Enter.

## Konfigurasi SSL

Konsep dasar melakukan caching situs HTTPS adalah proxy melakukan 3 hal berikut :

Klien request konten HTTPS > Situs memberikan VALID HTTPS konten > Proxy mendekripsi konten HTTPS tersebut untuk diinspeksi > Proxy menyematkan HTTPS palsu pada konten yang sudah dibuka diinspeksi tersebut > klien menerima konten HTTPS dari Proxy.

Proses penyematkan HTTPS palsu ini kita perlu membuat sertifikat SSL private milik si proxy kita sendiri. Berikut adalah cara-caranya :

```
# cd /etc/squid
# mkdir ssl_certs
# openssl genrsa -out squid.key 2048
# openssl req -new -key squid.key -out squid.csr -nodes
# openssl x509 -req -days 3652 -in squid.csr -signkey squid.key -out squid.crt
```

NB : Jika ada pertanyaan untuk mengisi nama company, organization dll, diikuti saja. Asal saat pengisian passphrase tidak usah, dikosongi saja.

Selanjutnya kita akan membuat direktori tempat penyimpanan cache sertifikat yang akan dibuat oleh

squid, pastikan tidak ada error yang muncul :

```
# mkdir /var/lib/squid
# chown -R nobody /var/lib/squid/
# /usr/lib/squid/ssl_crt -c -s /var/lib/squid/ssl_db
```

## Membuat Squid Autostart

Ini adalah langkah-langkah untuk membuat squid autostart setiap komputer hidup.

Pertama-tama download file script squid dengan perintah berikut :

```
# wget --no-check-certificate -O /etc/init.d/squid http://cilsy.id/upload/squid
# nano /etc/init.d/squid
```

*Ganti seluruh baris yang mengandung /proxy dengan direktori cache kalian masing-masing. Jika sudah simpan dan tutup file.*

Selanjutnya edit file berikut untuk membuat autostart :

```
# nano /etc/rc.local
```

Tambahkan ini sebelum baris exit 0 :

```
squid &
```

Simpan file.

## Konfigurasi File Log, Permission dan Hak Akses

Berikut adalah langkah-langkah untuk memastikan seluruh file-file log, permission, dan hak akses dari seluruh konfigurasi yang sudah kita lakukan sudah sesuai dengan ketentuan yang ada. Intinya agar tidak permission denied.

```
# mkdir /var/log/squid
# touch /var/log/squid/access.log
# chown -R proxy:proxy /etc/squid/squid.conf | chown -R proxy:proxy /usr/lib/squid | chown -R
proxy:proxy /var/lib/squid/ssl_db/certs | chown -R proxy:proxy /etc/squid/store-id.pl | chown -R
proxy:proxy /proxy | chown -R proxy:proxy /var/log/squid | chown -R proxy:proxy
/var/log/squid/access.log | chmod 777 /proxy | chmod 777 /var/log/squid | chmod 777
/var/log/squid/access.log | chmod 755 /var/lib/squid/ssl_db/certs | chmod +x /etc/init.d/squid
```

## Membuat Direktori Cache

Disini kita akan mengenerate direktori-direktori tempat penyimpanan cache proxy.

```
# squid -f /etc/squid/squid.conf -z
```

Tunggulah sebentar, setelah itu tekan CTRL + C untuk menyudahi. Kemudian ketikkan berikut :

```
# squid restart
```

Kemudian pastikan squid sudah running :

```
# service squid status
```

## Konfigurasi NAT dan Transparent Proxy

Ini untuk membelokkan traffic HTTPS dan HTTP klien ke proxy :

```
# nano /etc/rc.local
```

Isikan ini sebelum baris exit 0 dan baris squid &.

```
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
iptables -t nat -A POSTROUTING -s 192.168.30.0/24 -j MASQUERADE
iptables -I INPUT -p tcp -m tcp --dport 3129 -j ACCEPT
modprobe xt_TPROXY
modprobe xt_socket
modprobe xt_mark
modprobe nf_nat
modprobe nf_conntrack_ipv4
modprobe nf_conntrack
modprobe nf_defrag_ipv4
modprobe ipt_REDIRECT
modprobe iptable_nat
echo 1 > /proc/sys/net/ipv4/ip_forward
echo 0 > /proc/sys/net/ipv4/conf/default/rp_filter
echo 0 > /proc/sys/net/ipv4/conf/all/rp_filter
echo 0 > /proc/sys/net/ipv4/conf/lo/rp_filter
ip rule add fwmark 1 lookup 100
ip route add local 0.0.0.0/0 dev lo table 100
iptables -t mangle -F
iptables -t mangle -X
iptables -t mangle -N DIVERT
iptables -t mangle -A DIVERT -j MARK --set-mark 1
```

```
iptables -t mangle -A DIVERT -j ACCEPT
iptables -t mangle -A INPUT -j ACCEPT
iptables -t mangle -A PREROUTING -p tcp -m socket -j DIVERT
iptables -t mangle -A PREROUTING -d 192.168.88.100 -p tcp -m multiport --dports
22,80,443,3127,3128,3129,8000,8080,10000 -j ACCEPT
iptables -t mangle -A PREROUTING ! -d 192.168.88.100 -p tcp -m multiport --dports 80,8080,8000 -j
TPROXY --tproxy-mark 0x1/0x1 --on-port 3127
iptables -t mangle -A PREROUTING ! -d 192.168.88.100 -p tcp -m multiport --dports 443 -j TPROXY
--tproxy-mark 0x1/0x1 --on-port 3129
exit 0
```

*Ganti 192.168.88.100 menjadi ip eth0 kalian, dan ganti 192.168.30.0 dengan subnet jaringan lokal eth1 kalian.*

Jika sudah simpan file, dan coba restart komputer proxy.

# reboot

## Konfigurasi Sertifikat Klien

Salah satu hal yang harus dilakukan dalam melakukan caching HTTPS adalah kita harus menambahkan sertifikat squid kita ke browser di masing-masing klien agar proxy squid kita dipercaya oleh klien. Karena seperti yang sudah kita ketahui, konten yang diterima oleh klien sebenarnya sudah tidak original lagi. Jadi kita perlu memaksa klien agar tetap mempercayai konten-konten yang digenerate oleh proxy.

Caranya kalian buka aplikasi WINSCP, setelah itu remote ke proxy server :

```
Protocol : SCP
Hostname : 192.168.88.100
Username : rizal
Password : 123
```

Sesuaikan kondisi diatas dengan milik kalian masing-masing. Setelah itu kopikan semua file squid di /etc/squid/ssl\_certs ke komputer klien masing-masing.

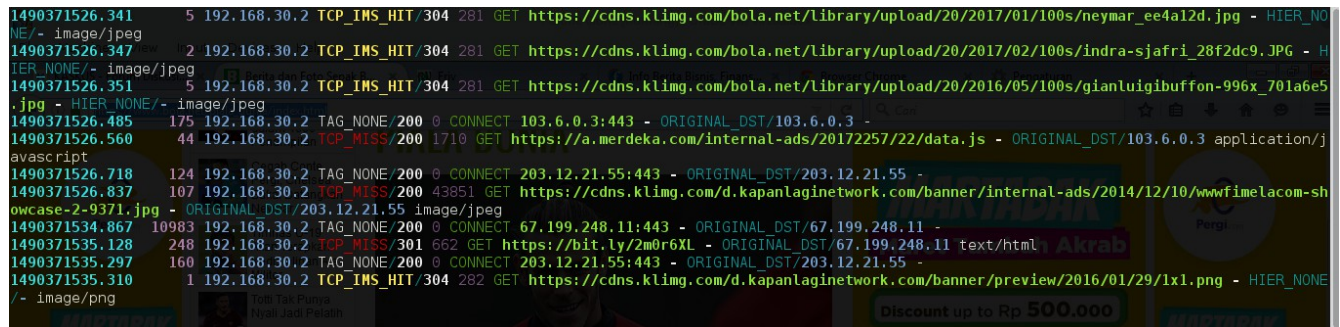
Kemudian buka browser di klien, masuk ke menu Options > Advanced > Certificate > View Certificate > Import. Centang semua opsi yang ada setelah itu klik Import.

## Testing Squid Proxy

Kalian bisa lihat log squid secara realtime dengan mengetikkan perintah berikut :

```
# tail -f /var/log/squid/access.log | ccze
```

Dari browser klien cobalah buka situs seperti bola.net atau detik.com atau kaskus.co.id lalu coba refresh halaman yang sudah pernah kalian akses. Maka seharusnya akan tampil banyak HIT.



```
1490371526.341 5 192.168.30.2 TCP_HIT/304 281 GET https://cdns.kling.com/bola.net/Library/upload/20/2017/01/100s/neymar_ee4a12d.jpg - HIER_NONE/- image/jpeg
1490371526.347 2 192.168.30.2 TCP_HIT/304 281 GET https://cdns.kling.com/bola.net/Library/upload/20/2017/02/100s/indra-sjafrir_28f2dc9.JPG - HIER_NONE/- image/jpeg
1490371526.351 5 192.168.30.2 TCP_HIT/304 281 GET https://cdns.kling.com/bola.net/Library/upload/20/2016/05/100s/gianluigibuffon-996x_701a6e5.jpg - HIER_NONE/- image/jpeg
1490371526.485 175 192.168.30.2 TAG_NONE/200 0 CONNECT 103.6.0.3:443 - ORIGINAL_DST/103.6.0.3 -
1490371526.560 44 192.168.30.2 TCP_MISS/200 1710 GET https://a.merdeka.com/internal-ads/20172257/22/data.js - ORIGINAL_DST/103.6.0.3 application/javascript
1490371526.718 124 192.168.30.2 TAG_NONE/200 0 CONNECT 203.12.21.55:443 - ORIGINAL_DST/203.12.21.55 -
1490371526.837 107 192.168.30.2 TCP_MISS/200 43851 GET https://cdns.kling.com/d.kapanlaginetwork.com/banner/internal-ads/2014/12/10/wwwfimelacom-showcase-2-9371.jpg - ORIGINAL_DST/203.12.21.55 image/jpeg
1490371534.867 10983 192.168.30.2 TAG_NONE/200 0 CONNECT 67.199.248.11:443 - ORIGINAL_DST/67.199.248.11 -
1490371535.128 248 192.168.30.2 TCP_MISS/301 662 GET https://bit.ly/2m0r6XL - ORIGINAL_DST/67.199.248.11 text/html
1490371535.297 160 192.168.30.2 TAG_NONE/200 0 CONNECT 203.12.21.55:443 - ORIGINAL_DST/203.12.21.55 -
1490371535.310 1 192.168.30.2 TCP_HIT/304 282 GET https://cdns.kling.com/d.kapanlaginetwork.com/banner/preview/2016/01/29/1x1.png - HIER_NONE/- image/png
```

## Konfigurasi Memblokir Situs Tertentu

Fungsi lain dari proxy squid adalah melakukan filtering konten. Contohnya kita dapat memblokir situs-situs tertentu maupun kata kunci tertentu yang tidak diinginkan. Caranya pertama-tama kita edit file /etc/squid/squid.conf :

```
# nano /etc/squid/squid.conf
```

Cari baris :

```
acl CONNECT method CONNECT
```

Tepat diatas baris tersebut, tambahkan :

```
acl terlarang url_regex -i "/etc/squid/terlarang.txt"
```

Ini berfungsi membuat ACL baru bernama terlarang yang letaknya ada di /etc/squid/terlarang.txt.

Setelah itu cari baris :

```
http_access allow localnet
```

Tepat diatas baris tersebut tambahkan :

```
http_access deny terlarang
```

Ini untuk memblokir ACL terlarang. Jika sudah simpan file squid.conf dengan menekan CTRL + X > Y > Enter.

Terakhir kita coba tambahkan list domain dan kata kunci yang ingin kita blokir dengan mengetikkan :

```
# nano /etc/squid/terlarang.txt
```

Didalamnya kalian isi misalnya :

```
youtube  
goal.com  
pintar
```

Jika sudah, simpan filenya.

Lalu restart squid dengan perintah :

```
# squid -k reconfigure
```

## Testing Pemblokiran Situs

Jika berhasil, seharusnya akan tampil halaman seperti ini saat pemblokiran terjadi :

