

Linux Proxy Server Dengan Squid dan Shorewall

Anton Picano Sanjaya
anton_picano@yahoo.com

Lisensi Dokumen:

Copyright © 2005 IlmuKomputer.Com

Seluruh dokumen di IlmuKomputer.Com dapat digunakan, dimodifikasi dan disebarkan secara bebas untuk tujuan bukan komersial (nonprofit), dengan syarat tidak menghapus atau merubah atribut penulis dan pernyataan copyright yang disertakan dalam setiap dokumen. Tidak diperbolehkan melakukan penulisan ulang, kecuali mendapatkan ijin terlebih dahulu dari IlmuKomputer.Com.

S Q U I D

Proxy server mempunyai kemampuan untuk menghemat bandwidth, meningkatkan keamanan dan mempercepat proses surfing web. Squid merupakan software proxy yang banyak dipakai dan dapat diperoleh secara gratis. Squid juga dapat digunakan untuk mengendalikan pemakaian bandwidth berdasarkan ekstensi file-file tertentu, menyaring situs-situs yang boleh diakses.

File-file yang dibutuhkan :

- Squid (yang dipakain pada tulisan ini adalah versi squid-2.5.STABLE6.tar.gz), bisa didownload dari <http://www.squid-cache.org>
- malloc.tar.gz, bisa didownload dari <http://www.gnu.org/order/ftp.html>

Instalasi dan konfigurasi

Ekstrak file squid hasil download ke direktori /usr/local/src

```
# tar xzvf squid-2.5.STABLE6.tar.gz -C /usr/local/src
```

Buat user untuk menjalankan squid

```
# useradd -d /cache/ -r -s /dev/null squid >/dev/null 2>&1
# mkdir /cache/
# chown -R squid.squid /cache/
# cd /usr/local/squid/squid-2.5.STABLE6
```

Edit file icons/Makefile.in, gantilah baris :

```
icondir=$(datadir)/icons
```

menjadi

```
icondir=$(libexecdir)/icons
```

Edit file src/Makefile.in, gantilah baris

```
DEFAULT_LOG_PREFIX = $(localstatedir)/logs
```

menjadi

```
DEFAULT_LOG_PREFIX = $(localstatedir)/log/squid

DEFAULT_PID_FILE = $(DEFAULT_LOG_PREFIX)/squid.pid

menjadi

DEFAULT_PID_FILE = $(localstatedir)/run/squid.pid


DEFAULT_SWAP_DIR = $(localstatedir)/cache

menjadi

DEFAULT_SWAP_DIR = /cache


DEFAULT_ICON_DIR = $(datadir)/icons

menjadi

DEFAULT_ICON_DIR = $(libexecdir)/icons
```

Editing file tersebut bertujuan untuk merubah lokasi default file `cache.log`, `access.log` dan `store.log` agar ditempat pada direktori `/var/log/squid` dan meletakkan PID squid pada direktori `/var/run` dan juga direktori icons `/usr/lib/squid/icons`.

GNU Malloc Library untuk Cache Performance Squid

Copy `malloc.tar.gz` ke direktori `/var/tmp`
`cp malloc.tar.gz /var/tmp`

Ektrak dan kompilasi malloc
`cd /var/tmp`
`tar zxvf malloc.tar.gz`
`cd malloc`
`make`

Copy library hasil kompilasi malloc (`libmalloc.a`) ke direktori lib
`cp libmalloc.a /usr/lib/libgnumalloc.a`

Copy file `malloc.h` ke direktori sistem include
`cp malloc.h /usr/include/gnumalloc.h`

Kompilasi Squid
`cd /usr/local/usr/squid-2.5.stable6`

`./configure \`
`--prefix=/usr \`
`--exec-prefix=/usr \`

```
--bindir=/usr/sbin \
--libexecdir=/usr/lib/squid \
--localstatedir=/var \
--sysconfdir=/etc/squid \
--enable-delay-pools \
--enable-cache-digests \
--enable-poll \
--disable-ident-lookups \
--enable-truncate \
--enable-storeio=diskd,ufs \
--enable-underscores \
--enable-err-languages=ENGLISH

# make
# make install
# mkdir -p /var/log/squid
# rm -rf /var/log/logs/
# chown squid.squid /var/log/squid/
# chmod 750 /var/log/squid/
# chmod 750 /cache/
# rm -f /usr/sbin/RunCache
# rm -f /usr/sbin/RunAccel
# strip /usr/sbin/squid
# strip /usr/lib/squid/unlinkd
# strip /usr/lib/squid/cachemgr.cgi
```

Buat script untuk menjalankan squid pada /etc/init.d dengan nama squid

```
#!/bin/bash
# squid          This shell script takes care of starting and stopping
#                Squid Internet Object Cache
#
# chkconfig: - 90 25
# description: Squid - Internet Object Cache. Internet object caching is \
# a way to store requested Internet objects (i.e., data available \
# via the HTTP, FTP, and gopher protocols) on a system closer to the \
# requesting site than to the source. Web browsers can then use the \
# local Squid cache as a proxy HTTP server, reducing access time as \
# well as bandwidth consumption.
# pidfile: /var/run/squid.pid
# config: /etc/squid/squid.conf

PATH=/usr/bin:/sbin:/bin:/usr/sbin
export PATH

# Source function library.
. /etc/rc.d/init.d/functions

# Source networking configuration.
. /etc/sysconfig/network

# Check that networking is up.
[ ${NETWORKING} = "no" ] && exit 0

# check if the squid conf file is present
[ -f /etc/squid/squid.conf ] || exit 0

if [ -f /etc/sysconfig/squid ]; then
. /etc/sysconfig/squid
else
SQUID_OPTS="-D"
SQUID_SHUTDOWN_TIMEOUT=100
fi
```

```
# determine the name of the squid binary
[ -f /usr/sbin/squid ] && SQUID=squid
[ -z "$SQUID" ] && exit 0

prog="$SQUID"

# determine which one is the cache swap directory
CACHE_SWAP=`sed -e 's/#.*//g' /etc/squid/squid.conf | \
    grep cache_dir | awk '{ print $3 }'`
[ -z "$CACHE_SWAP" ] && CACHE_SWAP=/var/lib/squid

RETVAL=0

start() {
    for adir in $CACHE_SWAP; do
        if [ ! -d $adir/00 ]; then
            echo -n "init_cache_dir $adir... "
            $SQUID -z -F 2>/dev/null
        fi
    done
    echo -n "Starting $prog: "
    $SQUID $SQUID_OPTS 2> /dev/null &
    RETVAL=$?
    [ $RETVAL -eq 0 ] && touch /var/lock/subsys/$SQUID
    [ $RETVAL -eq 0 ] && echo success
    [ $RETVAL -ne 0 ] && echo failure
    echo
    return $RETVAL
}

stop() {
    echo -n "Stopping $prog: "
    $SQUID -k check >/dev/null 2>&1
    RETVAL=$?
    if [ $RETVAL -eq 0 ] ; then
        $SQUID -k shutdown &
        rm -f /var/lock/subsys/$SQUID
        timeout=0
        while : ; do
            [ -f /var/run/squid.pid ] || break
            if [ $timeout -ge $SQUID_SHUTDOWN_TIMEOUT ]; then
                echo
                return 1
            fi
            sleep 2 && echo -n "."
            timeout=$((timeout+2))
        done
        echo success
        echo
    else
        echo failure
        echo
    fi
    return $RETVAL
}

reload() {
    $SQUID $SQUID_OPTS -k reconfigure
}

restart() {
    stop
    start
}

condrestart() {
    [ -e /var/lock/subsys/squid ] && restart || :
}

rhstatus() {
```

```
status $SQUID
$SQUID -k check
}

probe() {
    return 0
}

case "$1" in
start)
    start
    ;;
stop)
    stop
    ;;
reload)
    reload
    ;;
restart)
    restart
    ;;
condrestart)
    condrestart
    ;;
status)
    rhstatus
    ;;
probe)
    exit 0
    ;;
*)
    echo $"Usage: $0 {start|stop|status|reload|restart|condrestart}"
    exit 1
esac

exit $?
```

Rubah mode file /etc/init.d/squid
chmod +X /etc/init.d/squid

Edit file konfigurasi squid (/etc/squid/squid.conf)

```
# squid 2.5.Stable.x configuration
# by anton@ilmukomputer.com
#
#

http port 3128
icp_port 3130
udp_incoming_address 0.0.0.0
udp_outgoing_address 255.255.255.255
icp_query_timeout 0
maximum_icp_query_timeout 9000
mcast_icp_query_timeout 9000
hierarchy_stoplist cgi-bin ?
acl QUERY urlpath_regex cgi-bin \?
no_cache deny QUERY
cache mem 16 MB
cache swap low 80%
cache swap high 100%
maximum_object_size 1024 KB
minimum_object_size 4 KB
maximum_object_size_in_memory 8 KB
```

```
ipcache size 4096
ipcache low 90
ipcache high 95
fqdn_cache size 4096
cache replacement_policy lru
memory_replacement_policy lru
cache_dir diskd /cache 6000 14 256 Q1=64 Q2=72
cache_access_log /var/log/squid/access.log
cache_log /var/log/squid/cache.log
cache_store_log none
negative_ttl 2 minutes
emulate_httpd_log on
log_ip_on_direct on
pid_filename /var/run/squid.pid
debug_options ALL,1
log_fqdn off
client_netmask 255.255.255.255
ftp_user user@palanta.com
ftp_passive on
dns_retransmit_interval 5 seconds
dns_retransmit_interval 5 seconds
dns_timeout 5 minutes
diskd_program /usr/lib/squid/diskd
unlinkd_program /usr/lib/squid/unlinkd
redirect_rewrites_host_header on
request_header_max_size 10 KB
request_body_max_size 0 MB
auth_param basic children 5
auth_param basic realm Squid proxy-caching web server
auth_param basic credentialsttl 2 hours

refresh_pattern      \.(gif|jpg|jpeg)$      600 80% 86400
refresh_pattern      \.(xbm|xpm|ico|tiff)$    600 80% 86400
refresh_pattern      \.(au|snd|wav|ra|mid)$   600 80% 86400
refresh_pattern      \.(qt|mov|avi|mpeg)$     600 80% 86400
refresh_pattern      \.(iv|wrl|vrml)$        600 80% 86400
refresh_pattern      \.(Z|gz)$               600 80% 86400
refresh_pattern      \.(hqx|bin)$            600 80% 86400
refresh_pattern      \.(tar|zip)$            600 80% 86400
refresh_pattern      ^http://                30 50% 86400
refresh_pattern      ^ftp://                 30 50% 86400
refresh_pattern      .                        30 30% 43200

quick_abort_min 128 KB
quick_abort_max 4096 KB
quick_abort_pct 75
negative_ttl 1 minutes
range_offset_limit 0 KB
half_closed_clients off
shutdown_lifetime 30 seconds
acl all src 0.0.0.0/0.0.0.0
acl manager proto cache object
acl localhost src 127.0.0.1/255.255.255.255
acl to_localhost dst 127.0.0.0/8
acl boleh src 192.168.1.0/255.255.255.0
acl SSL_ports port 443 563
acl Safe_ports port 80          # http
acl Safe_ports port 21          # ftp
acl Safe_ports port 443 563    # https, snews
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 CONNECT method CONNECT
http_access allow manager localhost to localhost
http_access deny manager
http_access deny !Safe_ports
http_access allow boleh
```

```
http access deny all
icp access allow boleh
icp access deny all
reply body max size 0 allow all
cache mgr admin@palanta.com
cache_effective_user squid
cache_effective_group squid
visible hostname cache.palanta.com
httpd accel host virtual
httpd accel port 80
httpd accel single host off
httpd_accel_with_proxy on
httpd_accel_uses_host_header on
query icmp off
test reachability off
buffered logs on
reload into ims on
ie_refresh off
```

Jalankan squid

```
# /etc/init.d/squid start
```

SHOREWALL

Shorewall (Shoreline Firewall) merupakan firewall yang berbasis iptable yang dapat digunakan pada suatu sistem dedicated, gateway/router/server multifungsi atau pada standalone linux

File-file yang dibutuhkan

- shorewall-1.4.5-1.noarch.rpm, bisa di-download dari <http://www.shorewall.net/download.htm>
- netfilter/iptables
- iproute/iproute2

Instalasi

```
# rpm -ivh shorewall-1.4.5-1.noarch.rpm
# rm -f /etc/shorewall/startup_disable
```

Konfigurasi

/etc/shorewall/zone

File ini untuk mendefinisikan zona asal trafik pada jaringan

Isi file /etc/shorewall/zone :

```
#ZONE      DISPLAY      COMMENTS
net        Net          Internet
loc        Local        Local networks
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Server tempat shorewall diinstall dikenal sebagai zona yang disebut fw

/etc/shorewall/policy

File ini berisi aturan untuk semua traffic yang lewat pada firewall diatur pada /etc/shorewall/rules, jika tidak terdefiniskan pada file tersebut maka akan dicek pada /etc/shorewall/policy

```
#SOURCE ZONE      DESTINATION ZONE  POLICY      LOG      LIMIT:BURST
#                                     LEVEL
fw          net              ACCEPT
loc         net              ACCEPT
net         all              DROP
all         all              REJECT
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

/etc/shorewall/interface

File ini untuk menentukan interface yang akan terhubung dengan suatu zona

```
#ZONE      INTERFACE  BROADCAST  OPTIONS
net        eth0       detect     dhcp,norfc1918,blacklist
loc        eth1       detect
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

file diatas berarti eth0 terhubung dengan jaringan internet dan eth1 terhubung dengan jaringan lokal.

/etc/shorewall/masq

File ini untuk mendefinikan masquerade jaringan local dengan jaringan internet

Untuk mensetting apakah traffic yang melalui eth1 akan dibungkus (di-masquerade) dengan dengan IP pada eth0

```
#INTERFACE  SUBNET      ADDRESS
eth0  eth1
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

/etc/shorewall/rules

File ini berisi aturan-aturan dari semua traffic yang melewati firewall

```
# Rule dari local ke mesin (firewall)
# Terima koneksi DNS (Port 53)
ACCEPT loc fw tcp 53
ACCEPT loc fw udp 53

# Terima koneksi Proxy (Port 3128/8080)
ACCEPT loc fw tcp 3128
ACCEPT loc fw tcp 8080

# Terima koneksi Web (Port 80)
ACCEPT loc fw tcp 80

# Terima koneksi FTP (Port 20, 21)
ACCEPT loc fw tcp 20
ACCEPT loc fw tcp 21

# Terima koneksi SSH (Port 22)
ACCEPT loc fw tcp 22

# Terima koneksi Webmin (Port 10000)
ACCEPT loc fw tcp 10000

# Rule dari Internet ke mesin (firewall)
# Terima koneksi DNS
ACCEPT net fw tcp 53
ACCEPT net fw udp 53

# Terima koneksi SSH
ACCEPT net fw tcp 22
ACCEPT fw loc tcp 22

# Terima koneksi Web
ACCEPT net fw tcp 80

# Terima koneksi SMTP, POP3, IMAP
ACCEPT net fw tcp 25,110,143
ACCEPT fw net tcp 25,110,143
ACCEPT loc fw tcp 25,110,143
REJECT loc net tcp 25,110,143

# Terima koneksi Webmin
ACCEPT net fw tcp 10000
```

```
# Terima koneksi PING
ACCEPT  loc      fw      icmp    8
ACCEPT  net      fw      icmp    8
ACCEPT  fw       loc      icmp    8
ACCEPT  fw       net      icmp    8

# Redirect koneksi local port 80 ke port 3128
REDIRECT loc      3128    tcp      80

#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Jalankan shorewall

```
# /sbin/shorewall start
```

Referensi :

1. SQUID Frequently Asked Questions, <http://www.squid-cache.org>
2. Shorewall, Documentation, http://shorewall.net/Documentation_Index.html
3. Securing-Optimizing-Linux-The-Ultimate-Solution.pdf, <http://www.openna.com>