

Nama System : Proxy Server  
Versi : 1.0  
Bulan release : November 2008  
Manual oleh : Amin Yulianto, Web and System Administrator

# Proxy Server

# Installation Manual

## Table of Content:

Table of Content:.....	2
Preface.....	3
Purpose.....	3
Software used.....	3
Samples of screenshots:.....	3
Typography.....	4
Installation.....	5
Install CentOS 4.6 Minimal.....	5
Install Squid.....	5
Install adzapper.....	6
Install DansGuardian and ClamAV.....	6
OpenDNS + Bind.....	8
Access List (IPTables).....	9
Bibliography.....	10

## Preface

This manual is a how to setup a Proxy Server that will be used by all users for connecting to Internet. We will use an Open Source and/or free applications to achieves below requirement:

- Server is running on stable and updated OS
- Scan all traffic for virus
- Zap/remove all ads
- Content filtering based on naughtyness level and sites category

## Purpose

The purpose of this proxy server is:

- Maintain bandwidth usage for Internet
- Prevent virus spreading
- For keeping user productivity

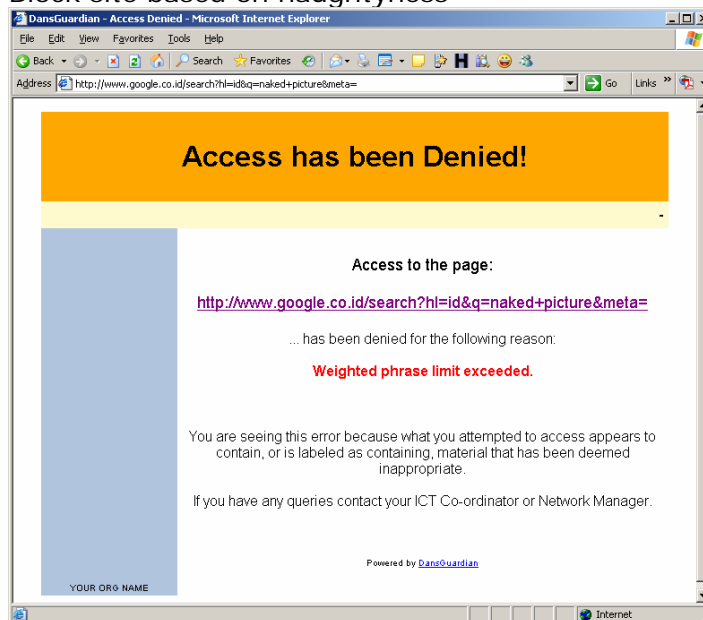
## Software used

Open source and/or free applications to create this proxy server are:

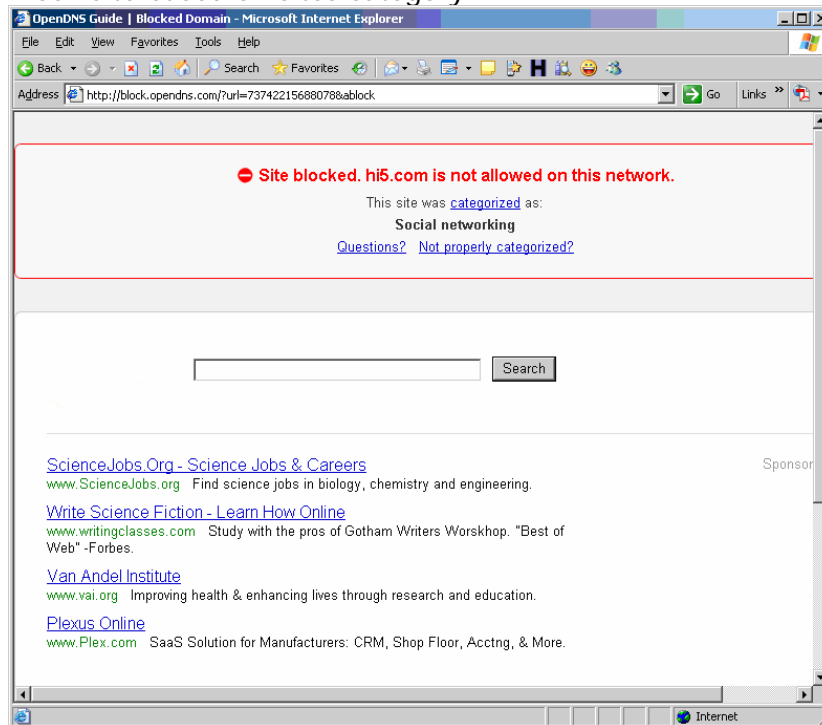
- CentOS – The Community ENTERprise Operating System
- Squid - Web Proxy Cache
- Adzapper – Ad Zapping with Squid
- DansGuardian - True Web Content Filtering for All
- ClamAV - open source (GPL) anti-virus toolkit for UNIX
- ISC BIND – Domain Name System server

## Samples of screenshots:

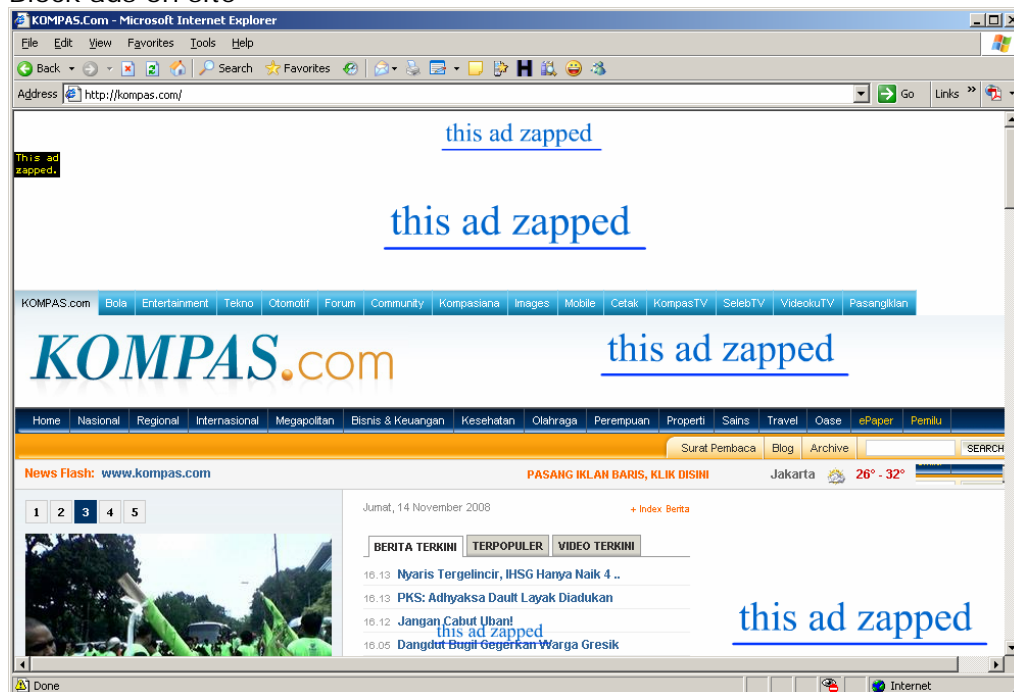
- Block site based on naughtyness



- Block site based on sites category



- Block ads on site



## Typography

- **bold phrase:** linux command
- *italic phrase:* content of a file and result of a command

All command executed as root user. IP Address of ProxyServer is 10.10.105.18

## Installation

### Install CentOS 4.6 Minimal

Install CentOS 4.6 with Minimal packages and use below configuration

- Disk partition:
  - /boot: 100MB
  - Swap partition: 2 x Memory size
  - / : rest of harddisk space
- Firewall: Disabled
- SELinux: Disabled

If you not specified the hostname for server at install time and want to change from localhost into something else (proxy.company.com) do it before configuring squid.

```
# vi /etc/sysconfig/network
NETWORKING=yes
HOSTNAME=proxy.company.com
# vi /etc/hosts
127.0.0.1 localhost.localdomain localhost
10.10.105.18 proxy.company.com proxy
```

### Install Squid

Make sure your server connected to Internet to get file from CentOS repository

```
# yum -y install squid
```

edit/change/add some variables on /etc/squid/squid.conf

```
# vi /etc/squid/squid.conf
cache_mem 128 MB
cache_dir ufs /var/spool/squid 4096 32 512
# Company ACL
acl Company src 10.10.0.0/16
# Company Rules
always_direct allow Company
# Allow/Disallow AIM connections
# Delete the following 9 lines if you don't want people to connect to AIM
#acl AIM_ports port 5190 9898 6667
#acl AIM_domains dstdomain .oscar.aol.com .blue.aol.com .freenode.net
#acl AIM_domains dstdomain .messaging.aol.com .aim.com
#acl AIM_hosts dstdomain login.oscar.aol.com login.glogin.messaging.aol.com toc.oscar.aol.com
irc.freenode.net
#acl AIM_nets dst 64.12.0.0/255.255.0.0
#acl AIM_methods method CONNECT
#http_access allow AIM_methods AIM_ports AIM_nets
#http_access allow AIM_methods AIM_ports AIM_hosts
#http_access allow AIM_methods AIM_ports AIM_domains
# Allow connections to Yahoo Messenger
# Delete the following 6 lines if you don't want people to connect to Yahoo Messenger
acl YIM_ports port 5050
acl YIM_domains dstdomain .yahoo.com .yahoo.co.jp
```

```

acl YIM_hosts dstdomain scs.msg.yahoo.com cs.yahoo.co.jp
acl YIM_methods method CONNECT
http_access allow YIM_methods YIM_ports YIM_hosts
http_access allow YIM_methods YIM_ports YIM_domains
# Allow connections to Google Talk
# Delete the following 6 lines if you don't want people to connect to Google Talk
#acl GTALK_ports port 5222 5050
#acl GTALK_domains dstdomain .google.com
#acl GTALK_hosts dstdomain talk.google.com
#acl GTALK_methods method CONNECT
#http_access allow GTALK_methods GTALK_ports GTALK_hosts
#http_access allow GTALK_methods GTALK_ports GTALK_domains
# Allow connections to MSN
# Delete the following 6 lines if you don't want people to connect to Google Talk
#acl MSN_ports port 1863 443 1503
#acl MSN_domains dstdomain .microsoft.com .hotmail.com .live.com .msft.net .msn.com .passport.com
#acl MSN_hosts dstdomain messenger.hotmail.com
#acl MSN_nets dst 207.46.111.0/255.255.255.0
#acl MSN_methods method CONNECT
#http_access allow MSN_methods MSN_ports MSN_hosts

```

Start and configure Squid at startup

```

# chkconfig squid on
# service squid start

```

## Install adzapper

```

get the latest version at http://adzapper.sourceforge.net
# wget http://adzapper.sourceforge.net/adzap-20080508.tar.gz
# tar xzvf adzap-20080508.tar.gz
# cp -R adzap /usr/local/
# vi /etc/squid/squid.conf
redirect_program /usr/local/adzap/scripts/squid_redirect
# crontab -e
0 2 * * 0 /usr/local/adzap/scripts/update-zapper

```

## Install DansGuardian and ClamAV

```

# rpm -ihv http://repo.securityteam.us/repository/redhat/securityteamus-repo-latest.rpm
# yum -y install dansguardian-av
# mv /etc/dansguardian/dansguardian.conf /etc/dansguardian/dansguardian.conf.old
# vi /etc/dansguardian/dansguardian.conf
reportinglevel = 3
langagedir = '/etc/dansguardian/languages'
language = 'ukenglish'
loglevel = 3
logexceptionhits = on
logfileformat = 1
loglocation = '/var/log/dansguardian/access.log'
filterip =
filterport = 8080
proxyip = 127.0.0.1
proxyport = 3128
accessdeniedaddress = 'http://YOURSERVER.YOURDOMAIN/cgi-bin/dansguardian.pl'

```

```
nonstandarddelimiter = on
usecustombannedimage = 1
custombannedimagefile = '/etc/dansguardian/transparent1x1.gif'
filtergroups = 1
filtergroupslist = '/etc/dansguardian/filtergroupslist'
bannediplist = '/etc/dansguardian/bannediplist'
exceptioniplist = '/etc/dansguardian/exceptioniplist'
banneduserlist = '/etc/dansguardian/banneduserlist'
exceptionuserlist = '/etc/dansguardian/exceptionuserlist'
showweightedfound = on
weightedphrasemode = 2
urlcachenumber = 3000
urlcacheage = 900
phrasefiltermode = 2
preservecase = 0
hexdecodecontent = 0
forcequicksearch = 0
reverseaddresslookups = off
reverseclientiplookups = off
createlistcachefiles = on
maxuploadsize = -1
maxcontentfiltersize = 256
usernameidmethodproxyauth = on
usernameidmethodident = off
preemptivebanning = on
forwardedfor = off
usexforwardedfor = off
logconnectionhandlingerrors = on
maxchildren = 120
minchildren = 8
minsparechildren = 4
preforkchildren = 6
maxsparechildren = 32
maxagechildren = 500
ipcfilename = '/tmp/.dguardianipc'
urlipcfilename = '/tmp/.dguardianurlipc'
pidfilename = '/var/run/dansguardian.pid'
nodaemon = off
nologger = off
daemonuser = 'nobody'
daemongroup = 'nobody'
softrestart = off
virusscan = on
virusengine = 'clamav'
tricklelength = 32768
forkscanlength = 32768
firsttrickledelay = 10
followingtrickledelay = 10
maxcontentscansize = 41904304
virusscanexceptions = on
urlcacheonly = on
virusscannertimeout = 60
notify = 2 # will notify the admin only
emaildomain = 'company.com'
postmaster = 'admin@company.com'
emailserver = '127.0.0.1:25'
```

```

downloadaddr = '/tmp/dgvirus'
clmaxfiles = 1500
clmaxrelevel = 3
clmaxfilesize = 10485760
clblockencryptedarchives = off
cldetectbroken = off
clamsocket = '127.0.0.1:3310'

```

Dont forget to change these lines with your own preferences.

```

accessdeniedaddress = 'http://YOURSERVER.YOURDOMAIN/cgi-bin/dansguardian.pl'
emaildomain = 'company.com'
postmaster = 'admin@company.com'

```

```

Start Dansguardian
# chkconfig dansguardian on
# service dansguardian start

```

Clamav packages on SecurityTeam.US repo is older (0.90) than current clamav version (0.94.1) which can cause dansguardion failed to start

```
# service dansguardian start
```

Starting Web Content Filter (dansguardian):

```
LibClamAV Warning: *****
```

```
LibClamAV Warning: *** This version of the ClamAV engine is outdated. ***
```

```
LibClamAV Warning: *** DON'T PANIC! Read http://www.clamav.net/support/faq ***
```

```
LibClamAV Warning: *****
```

```
[FAILED]
```

To fix it download latest clamav packages from <http://packages.sw.be/clamav/>

```
# wget http://packages.sw.be/clamav/clamav-db-0.94.1-1.el4.rf.i386.rpm
```

```
# wget http://packages.sw.be/clamav/clamav-0.94.1-1.el4.rf.i386.rpm
```

```
# wget http://packages.sw.be/clamav/clamd-0.94.1-1.el4.rf.i386.rpm
```

```
# rpm -Uh --force --nodeps clam*.rpm
```

```
# ln -s /usr/lib/libclamav.so.5 /usr/lib/libclamav.so.1
```

```
# service dansguardian start
```

## OpenDNS + Bind

Optional step to make your browsing experince safer and no bandwidth wasted

- Register with OpenDNS
- Add your Company network with OpenDNS.com
- Configure what filtering should be done by OpenDNS for my Company network in my case I choose custom and select below categories.

Adult Themes	Nudity
Adware	P2P/File sharing
Alcohol	Phishing
Dating	Photo sharing
Drugs	Podcasts
File storage	Pornography
Gambling	Proxy/Anonymizer
Games	Sexuality
Hate/Discrimination	Tasteless
Lingerie/Bikini	Video sharing
Movies	Weapons

- Add logo for OpenDNS and change comment (optional)

### Install Bind

```
# yum install bind caching-nameserver
# vi /etc/named.conf
options {
...
    forwarders { 208.67.222.222; 208.67.220.220; };
};
# vi /etc/hosts
127.0.0.1    localhost.localdomain localhost
10.10.105.18 newproxy.company.com newproxy

# vi /etc/resolv.conf
nameserver 127.0.0.1
```

### Start Bind

```
# chkconfig named on
# service named start
```

### Access List (IPTables)

Create access list for determining who can browse the internet (optional)

```
# vi /etc/sysconfig/iptables
*filter
:FORWARD ACCEPT [0:0]
:INPUT ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -p tcp -m tcp -s 10.10.105.100 -d 10.10.105.18 --dport 8080 -j ACCEPT
-A INPUT -p tcp -m tcp -s 10.10.104.95 -d 10.10.105.18 --dport 8080 -j ACCEPT
# SQUID CONFIG DO NOT DELETE!!!
-A INPUT -p tcp -m tcp -d 10.10.105.18 --dport 8080 -j DROP
COMMIT

*mangle
:FORWARD ACCEPT [0:0]
:INPUT ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:PREROUTING ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
COMMIT

*nat
:OUTPUT ACCEPT [0:0]
:PREROUTING ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
COMMIT
```

Start IPTables

```
# service iptables start
```

If you going to edit ACL just edit the file /etc/sysconfig/iptables then execute

```
# service iptables restart
```

## Bibliography

- [CentOS/RHEL : Web Proxy + Antivirus \(ClamAV\)](#)
- [How to configure squid proxy server using Fedora](#)
- [Ad Zapping with Squid](#)
- [DansGuardian - True Web Content Filtering for All](#)
- [Clam Antivirus](#)
- [OpenDNS – Providing A Safer And Faster Internet](#)