**SQUID PROXY CONFIGURATION GUIDE**

**ABSTRACT**

This “Do it yourself” guide is intended for any computer users who would like to improve theirinternet experience by creating local copies of frequently visited sites making them load faster whenrequested in future using Squid web cache.“Sharing copies of software is everybody's natural right and nobody should ever take that away”, saysRichard Stallman, Australia.Bill Gates once said, “the use of unauthorized copies of windows will get users addicted and eventuallyMicrosoft would find a way to charge them.”

**INTRODUCTION**

The need for the set up, configuration and deployment of a proxy server emanates from the need to improve the internet experience-getting better internet speeds or rather response times when requesting initially accessed web pages without necessary paying more to your ISP. This can be achieved bysetting up a proxy server within your local network which can cache previously accessed pages making them load faster when requested in future.

A proxy server receives requests from clients, searches within itself for the resource requested and if unavailable, the requests are forwarded to other servers on the internet. The responses are then cached prior to sending responses to client connected to it via a LAN.

The server may also have limited content filtering features that may allow one to limit access to certain resources perhaps totally or only grant access based on time, user of the system among other criteria chosen during the design of the content filter's access control lists.

Proxy servers are not only meant to be used by ISP's, large companies, research institutions and government institutions but may also be used in homes for instance to control what the children can access over the internet and the amount of time they can be on line on a given day besides accomplishing the improved speed satisfaction.

**REQUIREMENTS FOR SETTING UP SQUID PROXY SERVER**

Normally, a properly configured squid proxy server would not require high performance hardware system to run efficiently. However, the following portion below has to be put into consideration.

Squid proxy server requires a considerably large RAM; at least 512MB for a small organization. Low memory will significantly result in reduction in speed.

The other major consideration is disks. The faster the disk read and write speeds the faster squid will operate. As a result, SCSI disks are normally preferred just because of the speed. The other advantage of SCSI is that it can access seven different drives allowing for multiple reads and writes without a slowdown in access. SATA disks can however, be used as they considerably fast speeds, are cheap and are more readily available in larger sizes. ATA may be a poor option more so if they are on the same channel, as the system has to wait simply because only one disk can be accessed at a time.

**Choosing a suitable Operating System**

Assuming you are working on a shoe-string budget, we shall opt for “your freedom first”, as thecontroversial Richard Stallman puts it, stability, cost and the extent of support desired and thus, an opensource solution that is more secure and under which squid runs more efficiently than some proprietarysolutions available in the market, no malice intended whatsoever. We still need the proprietarysoftware.

There are a plethora of free and Open Source Linux distributions to choose from. The following are thefactors used to select CentOS(Community enterprise Operating System) as the distribution of choice:

1. It is stable

2. It is free

3. It is readily available for download

4. It is packaged with most applications required for the implementation of a proxy server.

5. It is a actively supported by its large community of users who mostly use it for server applications.

6. The Linux Community will always have security patches available even within an hour of discovering security vulnerabilities. Faster than what you get for the proprietary software as they normally have smaller teams working on their source code.

**Choosing a Proxy server application**

The proxy server of choice is Squid web proxy cache as it can both act as web cache and has minimalcontent-filtering features. Besides which it is free, well documented, rich in features and readilyavailable for download.

Other proxy servers that can be implemented on Linux are such as Oops, 3proxy which is freeware andipcorp which is still new in the market and not much information is presently available on the same.

**Configuring proxy server**

The following section describes the most frequently used options when configuring a squid proxyserver and as a result does not cover all the features that squid offers as this is beyond the scope of thisguide. This is probably going to be covered by someone else or probably is already covered.

**STEP I : Knowing your system**

It is necessary to know the Hardware architecture, Operating system and its release number, theapplication versions and the kernel number as some configurations may vary depending on any of theabove features. For instance, Squid version 2.6 and above configurations vary significantly that aperson whose previously used versions lower than 2.5 would not consider negligible.

These information is necessary and should be put into consideration when seeking for answers in Linuxforums, posting comments in blogs, mailing lists and other online communities. Below is a descriptionof how to obtain the above mentioned information:

**Operating System distribution and release**

The Linux distribution being used and its release can be retrieved prior to downloading of the diskimages. However, if the disks were downloaded by someone else or the system is already installed, one can normally obtain this information during installation and on start up of the installed system. Hence,our system will run on CentOS release 5.2 (final).

**Hardware architecture**

This may be categorized using bus-width, processor type etc. The most common architectures are:

a) x86 - This represents 32-bit systems and may be written as i386, i586, i686 and so forth.

b) x86-64 - This representation shows that a system has a 64-bit bus size.

**Checking if applications are installed and their versions**

This can be done on the terminal which can be accessed in the following manner. Go to

Applications >Accessories > Terminal to open gnome-terminal.

Alternatively, this can be accessed by pressing ALT+F2 to open the run application and typing in “gnome-terminal” followed by clicking on the Run button to run the terminal.



admin@server ~]$ rpm -q squid

squid-2.6.STABLE6-5.el5\_1.3

[admin@server ~]$

The above command shows that squid version 2.6 revision 6 is installed in release 5.2 of CentOS.

[admin@server ~]$ rpm -q iptablesiptables-1.3.5-4.el5

[admin@server ~]$

iptables version packaged in CentOS release 5.2 is version 1.3.5 and will be used in redirectingrequests from certain ports to the proxy server.

**Kernel version**

One can tell the kernel version using the uname command on the gnome terminal with the -r argumentas shown below to print the kernel version:

[admin@server ~]$ uname -r2.6.18-92.el5

[admin@server ~]$

Interpretation of the output above is the kernel in use is release 2.6.18 minor revision 92. The minorrevisions are specific or relevant to a given Linux distribution while the major version number isstandard across the Linux distributions.

It is in good practice that you upgrade the base operating system installed prior to commencing theconfiguration process. This will allow both the base system and the configurations to be updated unlikeattempting to upgrade an already configured system which would retain the configuration files.

**STEP II: Basic Configurations**

This section aims to get squid proxy to start successfully.

1. The first and critical step in configuring squid proxy server is confirming the existence of a default configuration file which is normally in the /etc/squid/ directory and backing it up. These can be done as shown in the following steps.

[admin@server ~]$ cd /etc/squid/

[admin@server squid]$ file squid.conf

squid.conf: ASCII English text

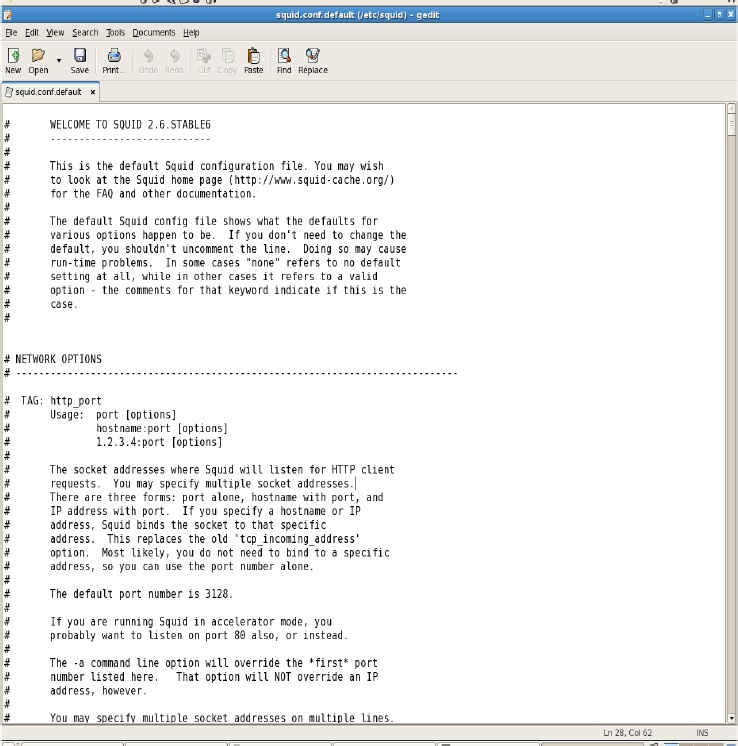
[admin@server squid]$ cp squid.conf squid.conf.default

[admin@server squid]$

**Interpretation:**

The first instruction changes the current directory to the directory where the squid configuration sits.After which the the next instruction checks the type of file squid.conf (default configuration file) is.Lastly, the default configuration file is backed up to squid.conf.default which can be used to restore thedefault configuration in the event of a failure.

The default squid configuration file looks as shown below when opened from gedit, a text editor.



The lines that commence with the hash(#) symbol are comments hence, are not read by the squiddaemon. The comments are include instructions and examples of how to make configurations.

2. Check that the port to which squid should listen for is configured. The default is port 3128.Whenever the redirecting application for instance the router or firewalling application sits onthe same server as the proxy then you only need to change the destination port to the port theproxy is listening on. This makes squid listen on a port rather than a socket as would be the casewhen we are redirecting requests from an external system. This is done as shown in the linebelow:

...Snippet from /etc/squid/squid.conf....................................................................................................

http\_port 3128

...Snippet from /etc/squid/squid.conf.....................................................................................................

3.Ensure that the cache\_dir is set to an exiting location

....Snippet from /etc/squid/squid.conf....................................................................................................

cache\_dir ufs /var/sqool/squid 100 16 256

...Snippet from /etc/squid/squid.conf....................................................................................................

where, 100 denotes a cache size of 100MB

For configuration purposes, let the default http\_access should be allowed to deny all connections thisline by default appears as shown below:

...Snippet from /etc/squid/squid.conf....................................................................................................

#Default:# http\_access deny all

...Snippet from /etc/squid/squid.conf....................................................................................................

To activate the above rule uncomment the line “http\_access deny all”. Note that “all” as used is anaccess control list that defines all ip addresses from any network. However, best practices would be tocopy the comment and append it below the comment to avail it for future reference or for the purposesof rollback in the case of erroneous alterations.

**STEP III: Start Squid**

Prior to starting squid proxy server, swap directories should be created. This can be done using theinstruction “squid -z” as a privileged user or as the super user.

[root@server admin]# squid –z

2009/06/15 09:01:20| Creating Swap Directories

[root@server admin]#

Once this is done, ensure squid service run as a user with adequate permissions to read and write to thecache directories and the log files.Finally, start squid using the following command:

[root@server admin]# /etc/rc.d/init.d/squid start

Starting squid: .................... [OK]

[root@server admin]#

These can also be done as follows:

[root@server admin]# /sbin/service squid start

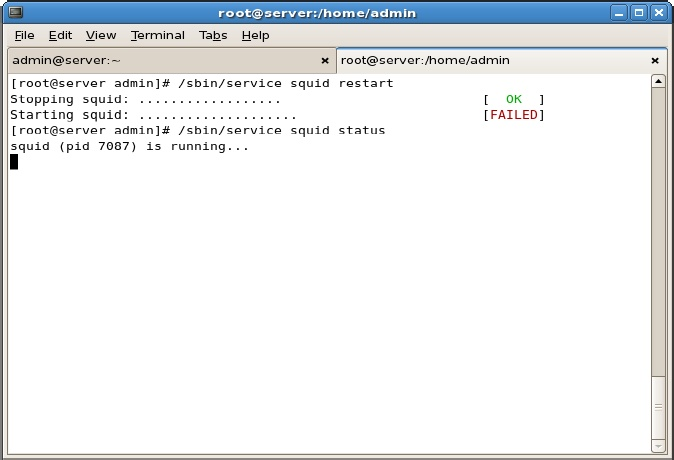
Starting squid: .................... [OK]

[root@server admin]#

To confirm that squid proxy server is running after start up, the status parameter may be sent to theservice command on specifying the service of interest as shown below:

[root@server admin]# /sbin/service squid status

squid (pid 5228) is running...This is necessary to do as squid 2.6 STABLE6 has a bug and by default would print out that start upfailed even when startup is successful, for example the following sequence of commands would outputas shown in the figure below:



The above described bug does not interfere with the running of squid and as a result may beoverlooked. This bug should have been corrected in subsequent releases currently being squid 3.x.

To configure squid to start every time the system starts up, the following command may be executed.

[root@server admin]# /sbin/chkconfig --level 345 squid on

[root@server admin]#

In the above command, the digits 3, 4 and 5 specify the run levels in which if the system boots into squid should run. Whereby, the default runlevel for squid is runlevel 5 which is the graphical modehowever, servers normally run in runlevel 3(text mode) which is more hardy and less prone to attacksand failure and it is for this reason preferred for servers.You can confirm that the configuration is effected using the following command:

[root@server admin]# /sbin/chkconfig --list squid

squid 0:off 1:off 2:off 3:on 4:on 5:on 6:off

[root@server admin]#

And as can be noted in the above output, Linux operating system normally has six distinct run levels whereby, the run levels symbolize the following states:

Run level State

1. Shutdown
2. Maintenance
3. <user / distribution defined>
4. Text-mode
5. <user / distribution defined>
6. Graphical-Mode
7. Restart

Run levels 2 and 4 by default are not configured however, may be configured to conform to the desiresof the user or as thought necessary by a given Linux community.

**STEP IV: Configure client browser**

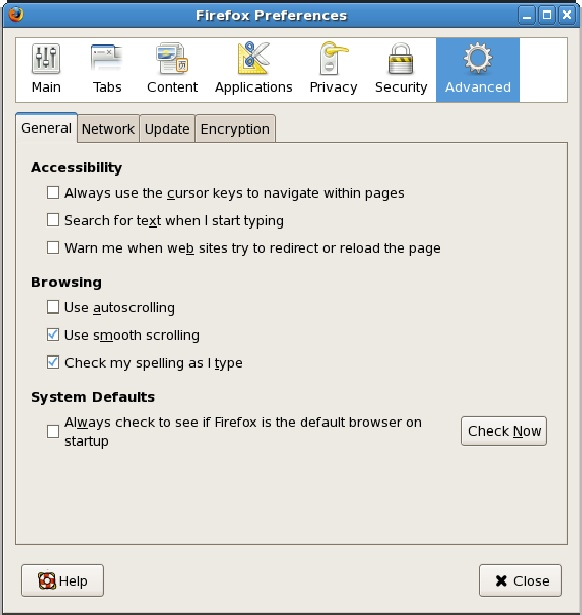
For this section, we shall use Mozilla Firefox 3.0.5 beta for illustration however, there exists a plethoraof other web browsers such as Safari, Internet explorer, Opera among others.

Procedure:

1. Click on the “Edit” menu on the browsers main menu.

2. Select the “Preferences” option.

3. On the pop up window, select “Advanced”



4. Select the “Network” tab.

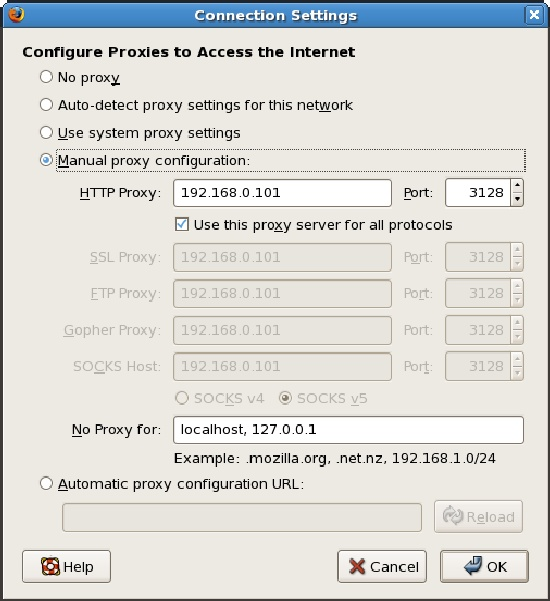


5. Select click the “Settings...” button

6. Select the “Manual proxy configuration” radio button

7. Enter proxy IP address and its ports number.

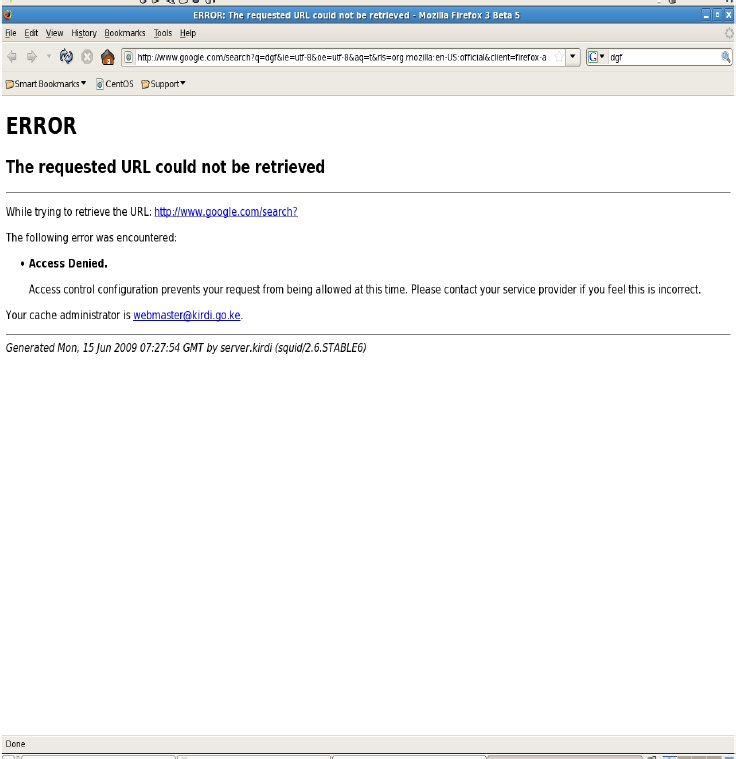
The resulting image should be as shown below:



The proxy setting for the squid server and the port that squid listens for connection are 192.168.0.101and 3128 respectively.

8.Restart the configuration to effect the new configuration.

Once the above configuration is done and squid is already running, an attempt to access a page on theInternet via your browser would result in the following page. Below, is the default error page which canbe tailored to suite the tastes of the organization such as shown later in this guide.



The error page displays the URL of the page that the client attempted to access, the email address of theperson to be contacted in case access is denied erroneously, date and time of denial and the name of theserver that hosts the squid process among others.

This error page may be modified to suit the preferences of a given organization or network in general.

**STEP III: Advanced Configurations**

Since we've confirmed that squid is running with the default ACL restriction (http\_access deny all)enforced, we shall proceed to the next stage of designing, testing and enforcing custom ACLs thatsatisfy the network needs for squid proxy.

**STEP I: Things to remember**

The ACL rule set are enforced / read from top to bottom . This means that if two rules contradict thefirst of the contradicting rules shall be enforced. In the example below, instruction number 3 holds truethus nobody shall be able to chat using google talk.

**REMEMBER**: The numbers are used for illustration and do not exist in the actual file

....Snippet from /etc/squid/squid.conf..............................................................................

1.acl google-talk port 5223 #XMPP over SSL

2.http\_access accept google-talk

3.http\_access deny google-talk

...Snippet from /etc/squid/squid.conf..............................................................................

You can join ACLs to form a single rule. For example, the below ruleset implies deny google talkaccess between Monday and Friday as from !0:00 a.m. To 2:00 p.m

...Snippet from /etc/squid/squid.conf............................................................................

acl google-talk port 5223#XMPP over SSL

acl working-hours time M T W H F 10:00-14:00

http\_access deny google-talk working-hours

...Snippet from /etc/squid/squid.conf............................................................................

Do not give ambiguity a chance. For instance, If a rule may stipulates, “allow clients on the MYNETnetwork to access the proxy server”. This is a valid rule and is not wrong by any standards butremember it doesn't specify what happens to those not in the MYNET network thus, those not in theMYNET network may still be able to access the proxy server. This ambiguity can be catered for bycreating a complimenting pair of rules.

E.g. http\_access allow MYNET

http\_access deny !MYNET

**Design and implementation of ACLs**

1.Write the rules in plain English

2.Convert them to ACLs using the supported squid acl types.

3.Concatenate ACLs where necessary to form a common rule.

For instance,

Only MYNET would use proxyMYNET proxy clients should not access the following sites: www.facebook.com, [www.myspace.com](http://www.myspace.com).

These would be converted to ACLs as follows:

acl MYNETWORK src 192.168.0.0/24

acl unwanted-sites url\_regex -i “/acl/unwanted-sites.txt”

where, the file unwanted-sites.acl would contain a list of the sites each in a new line. E.g. As shown below:

[www.facebook.com](http://www.facebook.com)

[www.myspace.com](http://www.myspace.com)

Finally, enforce the desired rules using the ACLs above created.

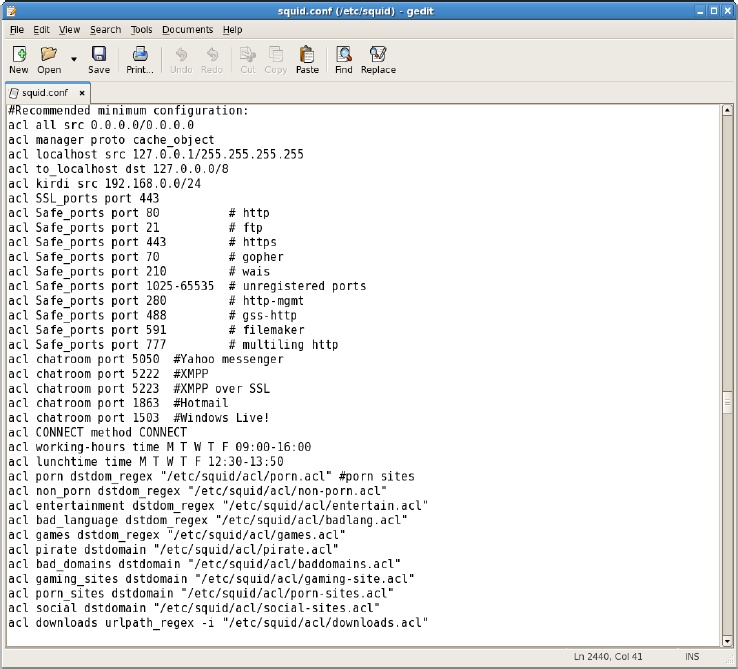
http\_access allow MYNETWORK

http\_access deny !MYNETWORK

http\_access deny unwanted-sites

For list type ACLs that require maintenance or updating from time to time, it is advisable to createthem in a text file to avoid making erroneous alterations during the process of updating ACLs. TheseACLs can the stored in a specified order to install order in our case, “/etc/squid/acl/”.

The ACLs that have been created on my squid proxy server are as shown below:



These ACLS are used to create the rules shown below:

...Snippet from /etc/squid/squid.conf................................................................................

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

http\_access deny porn

http\_access deny downloads

http\_access allow social lunchtime

http\_access deny social !lunchtime

http\_access allow non\_porn

http\_access allow MYNET

http\_access deny !MYNET

...Snippet from /etc/squid/squid.conf.................................................................................

A list of the resource to be filtered may appear as a regular ASCII text file as this shown below:

[root@server admin]# cat /etc/squid/acl/social-sites.acl

facebook.com

hi5.commyspace.com

[root@server admin]#

**Squid ACLs**

For the sake of order, we shall create a folder called

Acl inside the squid directory where we shall storeour ACLs. This we do as follows:

[root@server admin]# cd /etc/squid/

[root@server squid]# mkdir acl

[root@server squid]#

The ACLs used in this server can be categories into two:

a)Inline Acls

b)External ACLs

**a) Inline ACLs**

These are the ACLs defined within the file squid.conf some of them inlude:

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 127.0.0.0/8acl MYNET src 192.168.0.0/24

acl SSL\_ports port 443

acl Safe\_ports port 80 # http

acl Safe\_ports port 21 # ftp

acl Safe\_ports port 443 # https

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

acl working-hours time M T W T F 09:00-16:00

acl lunchtime time M T W T F 12:30-13:50

acl multimedia urlpath\_regex -i \.(mp3|avi|mpg|mpeg|asf|wmv|ra|rm|ram|asx|asf|afx|divx|m3u|viv|vivo|vo|flv|swf)$

**b) External ACLs**

These are ACL that are defined in external files for our scenario we store them in the directory,/etc/squid/acl . Squid can have ACLs of any extension as long as they are flat files.

**Streaming**

Streaming of multimedia has a tendency to grab large volumes of internet traffic thus, would result inslowed internet speeds. Multimedia are way larger and thus would require more bandwidth to theorganization. Since streaming wouldn't add value to the organization, blocking streaming would breakno bone.

acl streaming req\_mime\_type -i application/octet-stream

acl streaming req\_mime\_type -i application/x-mplayer2

acl streaming req\_mime\_type -i video/x-ms-asf

acl streaming req\_mime\_type -i audio/midi

acl streaming req\_mime\_type -i audio/mpeg

acl streaming req\_mime\_type -i video/x-msvideo

acl streaming req\_mime\_type -i video/x-flv

Streaming is blocked using mime-types as shown above however, and is blocked using http\_accessand http\_reply\_access as opposed to http request and this is shown below.

http\_access deny streaming

http\_reply\_access deny streaming

**Converting Squid to work in transparent caching mode**

STEP I: Configure Squid to listen for transparent connections

As of Squid version 2.6 the squid service can be made to work on transparent mode by simply appending the word transparent beside the proxy port number as shown below:

...Snippet from /etc/squid/squid.conf..................................................................................

http\_port 3128 transparent

...Snippet from /etc/squid/squid.conf.................................................................................

However, this is not all. We also need to configure iptables or a routes to redirect requests to the squidserver without making it necessary for one to make proxy configurations on the server clients. Thismakes it difficult for the clients to circumvent the proxy server by removing proxy configurations fromthe web browser they are using.

**STEP II: Configure iptables to support Squid**

Iptables is a RedHat Linux firewall application that could be used to redirect requests to the proxyserver. This can be done at the command line as follows:

[root@server admin]# iptables –F

[root@server admin]# iptables -t nat -F

[root@server admin]# iptables -t mangle –F

[root@server admin]# iptables -A INPUT -i eth0 -j ACCEPT

[root@server admin]# iptables -t nat -A PREROUTING -i ppp0 -p tcp --dport 80 -j REDIRECT --to-port 3128

[root@server admin]# iptables --table nat --append POSTROUTING --out-interface ppp0 –jMASQUERADE

[root@server admin]# service iptables save

iptables: Saving firewall rules to /etc/sysconfig/iptables:[OK]

In the configuration above, eth0 is the Network interface Card connected to the LAN whereas PPP0 isthe dial up modem that the squid server uses to connect to the internet. This configuration onlyredirects port 80 to the proxy server however, it should redirect all ports that should be filtered to theproxy server or the squid service to be precise.

The SSL port 443 and other secure communications should not be redirected to squid as the SSL keywould be altered and as a result no communication would occur as the host and client attempting tocommunicate would close session as they would detect this as a “man in the middle attack”. This issimply because squid does not support tunneling.

**Restoring iptables script**

One would be required to reload the configurations each time on rebooting the server using thefollowing command.

[root@server admin]# iptables-restore << /etc/sysconfig/iptables

However, this can be overcome by inserting the following line in the file /etc/rc.local using a text editorof choice and as a result the configuration would be automatically reloaded on restarting the system.The file will thus appear as shown below:

[root@server admin]# cat /etc/rc.local

#!/bin/sh

## This script will be executed \*after\* all the other init scripts.

# You can put your own initialization stuff in here if you don't

# want to do the full Sys V style init stuff.

touch /var/lock/subsys/local

iptables-restore /etc/sysconfig/iptables

[root@server admin]#

**Testing and Deployment**

To test that squid is operating in transparent mode which is technically known as intercepting proxymode since the requests are hijacked, remove the proxy configurations form the client initially beingused for testing and change the system gateway to the squid server IP address and then attempt toaccess a resource located on the Internet. If the results returned are those desired then your proxyserver is working alright.

**Squid logs and administration**

The squid proxy server may require regular administration to ensure it effectively filters content asdesired by the network administrators. This is necessary as the proxy clients are likely to identifyloopholes in the proxy configurations or even discover ways of circumventing the proxy server.

Updating of the ACL is necessary, and can be done with guidance from the squid generated logs thatinform the administrator of sites being visited, clients IP addresses, method used e.g. POST, GET, hostURL, action taken by the proxy server and the like.

**a)Access logs**

[root@server admin]# tail -f /var/log/squid/access.log

1245044255.491 0 192.168.0.240 TCP\_MISS/503 1630 GET

http://tracker.thepiratebay.org/announce? - DIRECT/tracker.thepiratebay.org text/html

1245044382.269 82742 192.168.0.240 TCP\_MISS/503 1626 GET

http://tracker.thepiratebay.org/scrape? - DIRECT/tracker.thepiratebay.org text/html

1245044382.269 66439 192.168.0.240 TCP\_MISS/503 1630 GET

http://tracker.thepiratebay.org/announce? - DIRECT/tracker.thepiratebay.org text/html

1245044585.260 82105 192.168.0.240 TCP\_MISS/503 1630 GET

http://tracker.thepiratebay.org/announce? - DIRECT/tracker.thepiratebay.org text/html

1245044592.423 1 192.168.0.240 TCP\_MISS/503 1630 GET

http://tracker.thepiratebay.org/announce? - DIRECT/tracker.thepiratebay.org text/html

1245044605.450 1 192.168.0.240 TCP\_MISS/503 1626 GET http://tracker.thepiratebay.org/scrape?- DIRECT/tracker.thepiratebay.org text/html

1245044658.257 91210 192.168.0.240 TCP\_MISS/503 1630 GET http://weather.noaa.gov/cgi-bin/mgetmetar.pl? - DIRECT/weather.noaa.gov text/html

1245044908.245 82174 192.168.0.240 TCP\_MISS/503 1630 GET

http://tracker.thepiratebay.org/announce? - DIRECT/tracker.thepiratebay.org text/html

1245050874.281 0 192.168.0.101 TCP\_DENIED/403 1458 GET http://www.google.com/search? -NONE/- text/html

**b)Cache logs**

[root@server admin]# tail -f /var/log/squid/cache.log

2009/06/15 10:27:07| 0 Objects expired.

2009/06/15 10:27:07| 0 Objects cancelled.

2009/06/15 10:27:07| 0 Duplicate URLs purged.

2009/06/15 10:27:07| 0 Swapfile clashes avoided.

2009/06/15 10:27:07| Took 26.2 seconds ( 4.8 objects/sec).

2009/06/15 10:27:07| Beginning Validation Procedure

2009/06/15 10:27:07| Completed Validation Procedure

2009/06/15 10:27:07| Validated 126 Entries

2009/06/15 10:27:07| store\_swap\_size = 744k

2009/06/15 10:27:08| storeLateRelease: released 0 objects

These logs are a very vital part of proxy administration and can help identify configuration loop holesand unhandled sections prior to any reports being made by the clients.

**SUMMARY AND CONCLUSION**

A well configured proxy is very valuable to an organization however, a poorly configured proxy server may present greater risks than in the absence of one thus, great care is necessary while setting up a proxy server.

Squid is free and Open Source and is even better than most proprietary proxy servers in the market. Its major flaw is the need for technical know how unlike the proprietary solutions which have easy to use interfaces thus making them easier to configure and deploy.

There exist Graphical User Interfaces for configuring squid thus making it easier to configure. However, great care is needed when choosing the right one to use as some delete the default configuration file and create custom ones which in some cases may make squid to fail to start.