UNIVERSITY OF MAURITIUS

Faculty of ICDT

Department of ICT

Module: Computer Networks and System Administration (ICT 3053Y)
Lab sheet 1: Semester 2 (indicative duration: 2 weeks)
Aims: Setting Up Proxy Server on CentOS Linux: Caching, Filtering by URL's, Filtering by Keywords
Compiled by: Dr. J. Seetohul

A proxy server is a computer which sits between two endpoint devices and acts as an intermediate device. When the client computer requests a resource from the server, it may be a file or a web page, the request is sent to the proxy server first. The proxy server then sends the request to the destination server and obtains the resource sent by the server.

Once the resource is obtained by the proxy server, it sends the resource to the client machine. The use of a proxy server is that it can cache the resource, for example if a website is accessed frequently from a proxy server, it's likely that the proxy server will have the content of the site in its cache, it can now serve the webpage directly to the user. A proxy server can be used to facilitate security, administrative controls and caching services. Proxy servers can also be used for anonymity as whenever obtaining a resource from a server, proxy server uses its own IP address rather than the client's IP address.

Squid Proxy is an open source caching proxy for the web. It supports many protocols such as HTTP, HTTPS, FTP and more. It improves the response time and reduces bandwidth by caching and reusing the frequently accessed web pages and files. In this tutorial we will learn to install Squid Proxy on CentOS 7. We will also learn about some basic configuration which can be done on Squid caching server.

First get acquainted to the following ACL (Access Control List) types:

srcdomain: source (client) domain name
dstdomain: destination (server) domain name
url_regex: URL regular expression pattern matching

Requirements

Squid does not have any minimum hardware requirements, but the amount of RAM may vary according to the users accessing the Internet through your proxy and the objects stored in the cache. To follow this tutorial you will need a CentOS 7.x server with root access on it. If you are logged in as non-root user, run #sudo -i to switch to root user. You can also use sudo command before all the administrative commands to run them as root user.

Installing Squid

You will need to install EPEL repository to your system as Squid is not available in default yum repository. Run the following command to install EPEL repository in your server.

#yum -y install epel-release
#yum clean all

Now you can install Squid Proxy using the following command.

#yum -y install squid

Next, update openssl

#yum -y update openssl

Once you have installed Squid, you can start the program immediately using the following command.

#systemctl start squid (or alternatively #service squid start)

You can check the error logs of Squid using the following command.

#tail -f /var/log/squid/access.log

Configuring Squid

Squid can be easily configured by editing the global configuration file /etc/squid/squid.conf. To edit the configuration file run the following command.

#gedit /etc/squid/squid.conf

Allowing Your Subnet to use the Internet through Your Proxy Server

To allow a range of IP addresses from your subnet to use the Internet through your proxy server. You can add a new ACL entry. Squid supports CIDR notations. For example,

acl localnet src 196.168.46.0/24

Your list of ACLs will finally look like this.

```
    acl localnet src 10.0.0.0/8     # RFC1918 possible internal
network
    acl localnet src 172.16.0.0/12  # RFC1918 possible internal
network
    acl localnet src 192.168.0.0/16 # RFC1918 possible internal
network
    acl localnet src fc00::/7       # RFC 4193 local private network
range
    acl localnet src fe80::/10      # RFC 4291 link-local (directly
plugged) machines
    acl localnet src 196.168.46.0/24 #Your newly added ACL
```

For changes to take effect you will need to restart your Squid server, use the following command for same.

#systemctl restart squid (or #service squid restart)

Configuring Squid Proxy as a Web Filter

You can restrict user access to particular websites or keywords using Access Control Lists (ACLs).

1. Restricting Access to Specific Web Sites

We can see how to block itworld.com and easy.com .

Step 1 » create a file blockedsites.squid in /etc/squid.

gedit /etc/squid/blockedsites.squid and add the web site names **one per line**

#blocked sites

.itworld.com (or www. itworld.com)

.easy.com (or www. easy.com)

Step 2 » Open the /etc/squid/squid.conf and create a new acl "blocksites" and acl type "dstdomain" in the acl section as shown below .

```
1 acl Safe_ports port 488       # gss-http
2 acl Safe_ports port 591       # filemaker
3 acl Safe_ports port 777       # multiling http
4 acl CONNECT method CONNECT
5 # ACL blocksites
6 acl blocksites dstdomain "/etc/squid/blockedsites.squid"
```

Now add the following line "http_access deny blocksites" to http_section to deny the access to the acl "blocksites"

 # Recommended minimum Access Permission configuration:

```
#
# Only allow cachemgr access from localhost
http_access allow manager localhost
# Deny access to blocksites ACL
http_access deny blocksites
http_access deny CONNECT blocksites
```

Step 3 » Now restart squid service

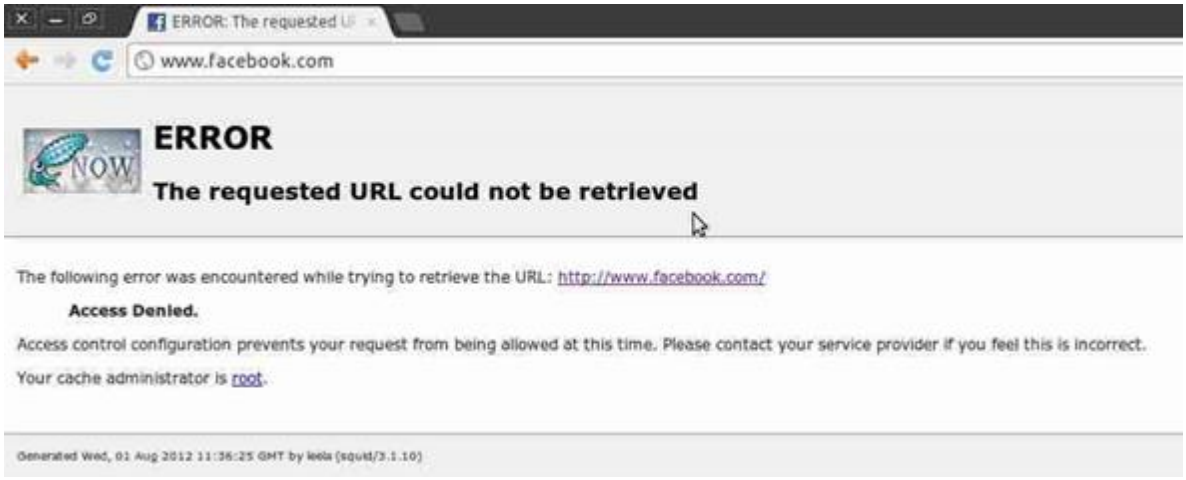
systemctl restart squid (or service squid restart or service squid reload)

Step 4 » **Setup your web browser to access Internet through proxy server on port 3128**

Internet Explorer: Tools » Internet options »Connections » LAN settings » Choose "Use a proxy server for your LAN" » Type your Proxy Server IP (192.168.1.11) and port no 3128

Firefox: Options/Preferences » Advanced » Network » Settings » Choose "Manual proxy configuration " » Type your Proxy Server's IP (192.168.1.11) and port no 3128

Step 5 » Try to access itowrld.com in your browser - you could see the blocked page.



You may wish to edit the error message generated by squid by editing the ERR_ACCESS_DENIED and provide a more elegant message of your own choice.
gedit /usr/share/squid/errors/en/ERR_ACCESS_DENIED
Enter your own error message now.

Check the log file you can see the itworld.com request is denied.
tail -f /var/log/squid/access.log

NOTE WELL: An alternative and yet simple way to restrict access to web sites is to enter the websites to be blocked directly in the squid.conf file (without having to create the blockedsites.squid file and entering the websites to be blocked line by line in it as it has been done above). Here is an example.
acl blocksite dstdomain .lycos.com .itworld.com .youtube.com .facebook.com
http_access deny blocksite
Note: by placing a dot before lycos.com (or facebook.com), http://www.lycos.com or www.lycos.com or simply lycos.com will be also blocked. The same applied for facebook (secure http) – facebook.com or www.facebook.com or https://www.facebook.com will ALL be blocked.

2. Restricting Access to Specific Keywords

Step 1 » create a file blockkeywords.squid in /etc/squid/.
#gedit /etc/squid/blockkeywords.squid and enter the following keywords **one per line**
#blocked keywords
FOOTBALL
football
BOLLYWOOD
bollywood
TENNIS
tennis

Step 2 » Open the /etc/squid/squid.conf and create a new acl “blockkeywords” and acl type “url_regex” in the acl section

```
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 blocksites
acl blocksites dstdomain "/etc/squid/blockedsites.squid"
# ACL blockkeywords
acl blockkeywords url_regex -i "/etc/squid/blockkeywords.squid"
```

Now add the following line “http_access deny blockkeywords” to http_section to deny the access to the acl “blockkeywords”.

```
# Recommended minimum Access Permission configuration:
#
# Only allow cachemgr access from localhost
http_access allow manager localhost
# Deny access to blocksites ACL
http_access deny blocksites
# Deny access to blockkeywords ACL
http_access deny blockkeywords
```

Step 3 » Restart squid and test using your browser

NOTE WELL: An alternative and yet simple way to restrict access to specific keywords is to enter the keywords to be blocked directly in the squid.conf file (without having to create the blockkeywords.squid file and entering the keywords to be blocked line by line in it as it has been done above). Here is an example.

```
acl blockkeyword url_regex football bollywood games
http_access deny blockkeyword all
```

NOTE: The url_regex means to search the entire URL for the regular expression you specify. Note that these regular expressions are case-sensitive, so a url containing the "football" in the keywordlist file will be denied while “FOOTBALL” would be allowed.

3. Restricting Access to specific IP Addresses

Step 1 » create a file blockip.squid in /etc/squid/

#gedit /etc/squid/blockip.squid and add the IP addresses **one per line**.

```
#blocked ips
192.168.1.20
192.168.1.21
```

Step 2 » Open the /etc/squid/squid.conf and create a new acl “blockip” and acl type “src” in the acl section

```
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 blocksites
acl blocksites dstdomain "/etc/squid/blockedsites.squid"
# ACL blockkeywords
acl blockkeywords url_regex -i "/etc/squid/blockkeywords.squid"
# ACL blockip
acl blockip src "/etc/squid/blockip.squid"
```

Now add the following line “http_access deny blockip” to http_section to deny the access to the acl “blockip”

```
# Recommended minimum Access Permission configuration:
#
# Only allow cachemgr access from localhost
http_access allow manager localhost
# Deny access to blockip ACL
http_access deny blockip
# Deny access to blocksites ACL
http_access deny blocksites
# Deny access to blockkeywords ACL
http_access deny blockkeywords
```

Step 3 » Restart squid and test using your browser

4. Allow Full Access to Specific IP Address

You can allow specific ip address to gain full access without blocking sites and keywords.
Create a file allowip.squid in /etc/squid/ and add the IP address one per line and create an acl “allowip” and acl type “src” in the acl section.

```
# ACL allowip
acl allowip src "/etc/squid/allowip.squid"
```

Now add the “allowip” in the http_access as shown below

```
# Recommended minimum Access Permission configuration:
#
# Only allow cachemgr access from localhost
http_access allow manager localhost
# Deny access to blockip ACL
http_access deny blockip
# Deny access to blocksites ACL
```

http_access deny blocksites !allowip
Deny access to blockkeywords ACL
http_access deny blockkeywords !allowip

5. Changing Squid Proxy Port Number (OPTIONAL – DO NOT USE)

You can change squid proxy port number - by default it uses port 3128.
Just find the line below in "/etc/squid/squid.conf"
http_port 3128
and replace with
http_port 8000 # or whatever port number you want

6. Restricting Download Size

You can restrict download file size using reply_body_max_size .
Add the line below **at the bottom of the http_access section**
#Restrict download size
reply_body_max_size 10 MB all
or
#Restrict download size
reply_body_max_size 10 MB !allowip

Troubleshooting Squid

If you not able to browse using proxy settings, disable the firewall (iptables) and selinux service on your squid proxy server.

Disable firewall (iptables)

#service iptables stop
chkconfig iptables off

Disable Selinux

Open the file /etc/selinux/config and find the line
SELINUX=enforcing
and replace with
SELINUX=disabled

NOTE: To enforce "pure" filtering by keyword (content filtering by searches made using a specific keyword), it is best to install and configure squidguard, which is available at:
http://www.squidguard.org
Choose the currently available stable version.

FOR FUTURE USE

How do i allow clients/users to use the cache?

Define an ACL that corresponds to clients' IP addresses. For example:
acl myclients src 192.168.126.0/24
Next, allow those clients in the http_access list:
http_access allow myclients

How do i configure squid NOT to cache a specific server?

acl someserver dstdomain .thatserver.com
cache deny someserver

Allowing Internet to Everyone Except for a Particular Machine (used by Bad Employee)

All what we need to do is to block the machine's IP Address
Open squid.conf and add the following lines

acl bad_employee src 192.168.1.18
http_access deny bad_employee
acl mynetwork src 192.168.1.0/24
http access allow mynetwork

In the above example the entire network will be allowed to use the internet except the blocked person's (bad_employee) machine. Remember Squid interprets the rules from top to bottom, so you need to be careful.

Creating a Restricting Rule by TIME Allowed

Open squid.conf and add the following lines
acl mynetwork src 192.168.1.0/24
acl business_hours time M T W H F 9:00-17:00
acl bad_employee src 192.168.1.18
http_access deny bad_employee
http_access allow mynetwork business_hours

Blocking Downloads of .exe files

Open squid.conf and add the following lines
acl block_exe url_regex .*\.exe$
http_access deny block_exe
If you want block more extensions to download, you can specify all in a file as described above (just as done in the URL block section).

Blocking TLDs (for example: .br .eu)

Open squid.conf and add the following lines
acl block_tld dstdom_regex \.br$
http_access deny block_tld