Department of Information Technology

Academic Year: 2022-23 **Semester: V**
Class / Branch: TE IT Subject: Security Lab (SL)
Subject Lab Incharge: Prof. Apeksha Mohite

Experiment No. 2

1. Aim: To study access control list by configuring SQUID proxy server.

2. Theory:

Proxy servers operate as an intermediary between a local network and services available on a larger one such as the Internet. Requests from local clients for web services can be handled by the proxy server, speeding transactions as well as controlling access. Proxy servers maintain current copies of commonly accessed web pages, speeding web access times by eliminating the need to access the original site constantly. They also perform security functions, protecting servers from unauthorized access. Squid is a free, open source, proxy-caching server for web clients, designed to speed Internet access and provide security controls for web servers. Copies of web pages accessed by users are kept in the Squid cache, and as requests are made, Squid checks to see if it has a current copy. If Squid does have a current copy, it returns the copy from its cache instead of querying the original site. If it does not have a current copy, it will retrieve one from the originalsite. In this way, web browsers can then use the local Squid cache as a proxy HTTP server. Squid currently handles web pages supporting the HTTP, FTP, and SSL protocols.

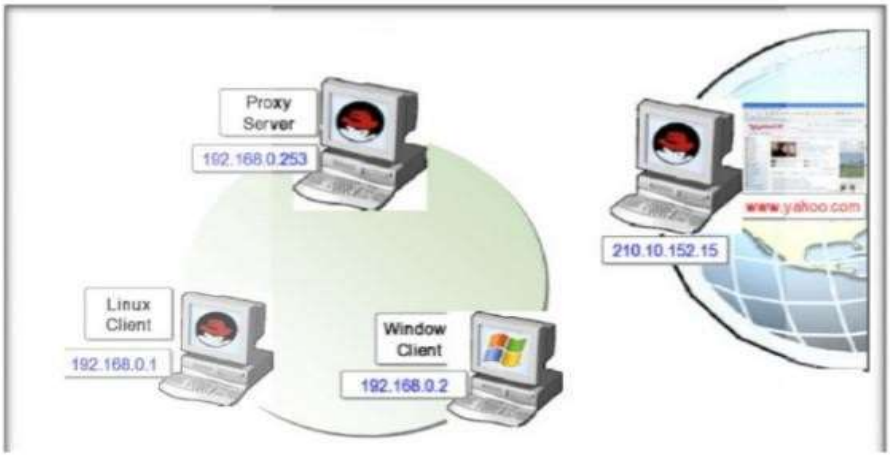
Requirement of squid proxy server can be summarized by following points:

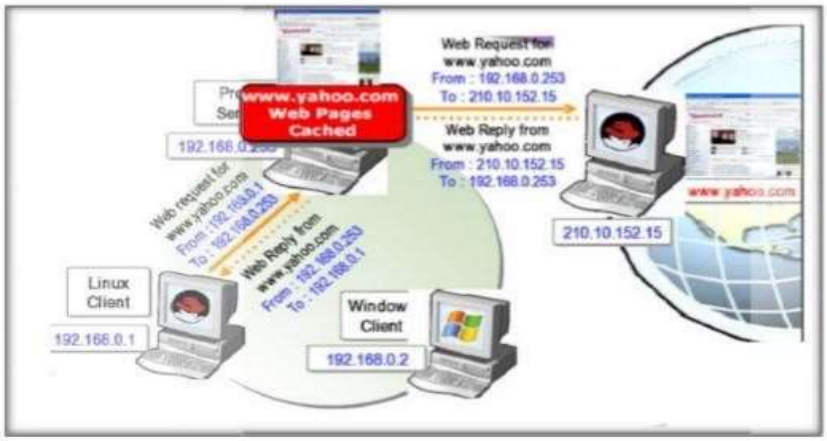
1. Squid stores files from previous requests to speed up future transfers. For example, suppose

client1downloads CentOS-7.0-1406-x86_64-DVD.iso from Internet. When client2 requests access to the same file, squid can transfer the file from its cache instead of downloading it again from the Internet. This feature can be used to speed up data transfers in a network of computers that require frequent updates of some kind.

2. ACLs (Access Control Lists) allow us to restrict the access to websites, and / or monitor the access on a per user basis. Access can be restricted based on day of week or time of day, or domain.

3. Bypassing web filters is made possible through the use of a web proxy to which requests are made and which returns requested content to a client, instead of having the client request it directly to the Internet.





The access control scheme of the Squid web proxy server consists of two different components:

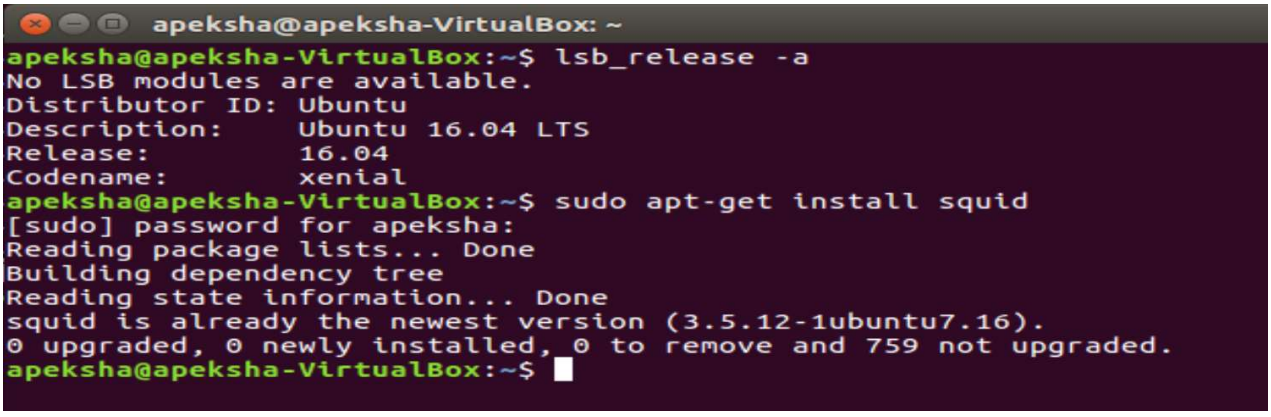
1. The ACL elements are directive lines that begin with the word "acl" and represent types of tests that are performed against any request transaction.

2. The access list rules consist of an allow or deny action followed by a number of ACL elements, and are used to indicate what action or limitation has to be enforced for a given request. They are checked in order, and list searching terminates as soon as one of the rules is a match. If a rule has multiple ACL elements, it is implemented as a boolean AND operation (all ACL elements of the rule must be a match in order for the rule to be a match).

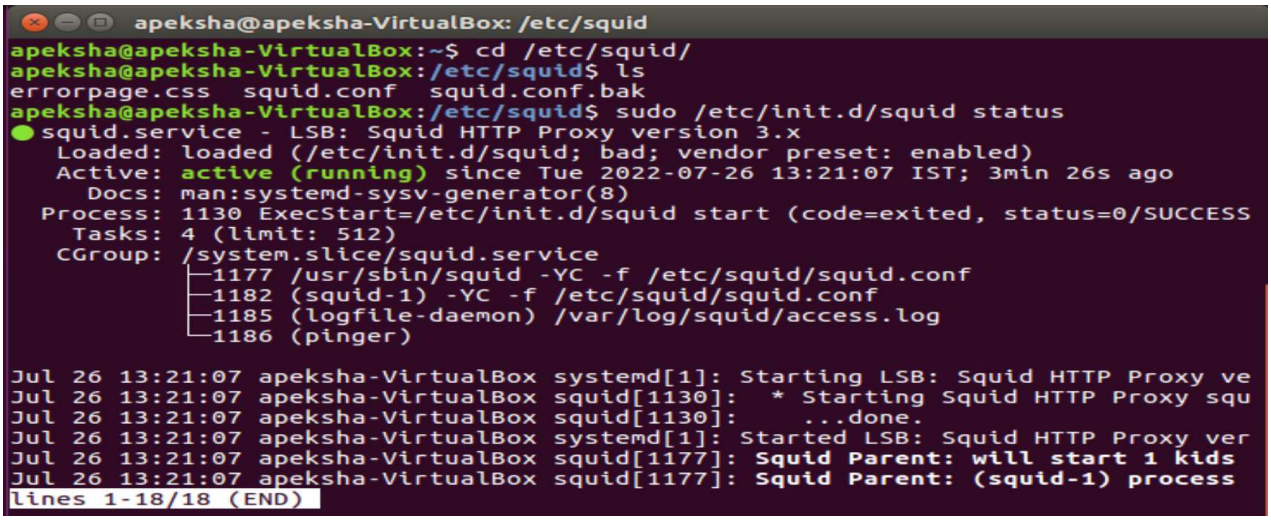
Squid's main configuration file is /etc/squid/squid.conf, which is 5000 lines long since it includes both configuration directives and documentation. For that reason, new squid.conf file can be created with only the lines that include configuration directives for our convenience, leaving out empty or commented lines. To do so, following commands can be used

Installation of SQUID:

Command : sudo apt-get install squid

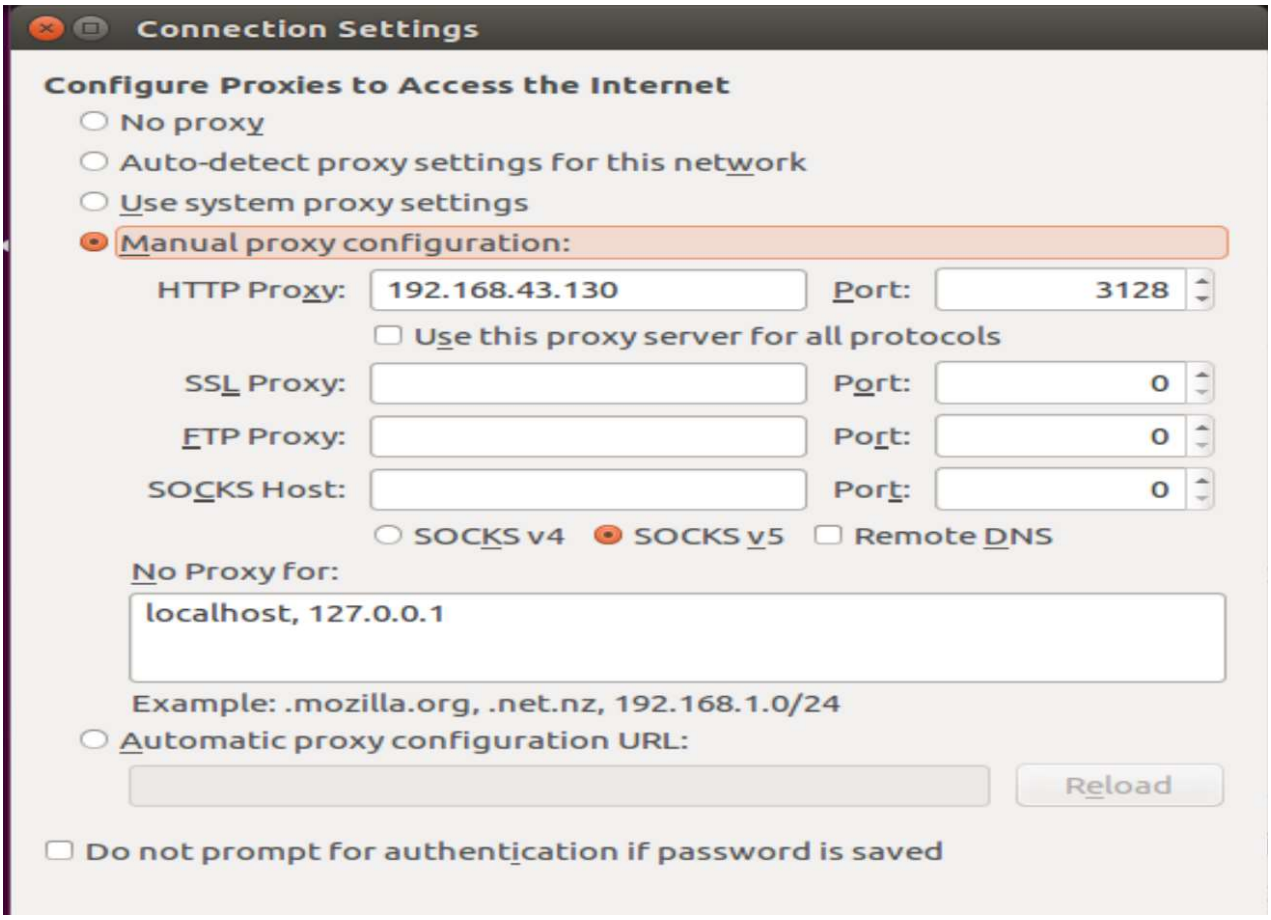


Check status of SQUID :



Firefox Proxy settings

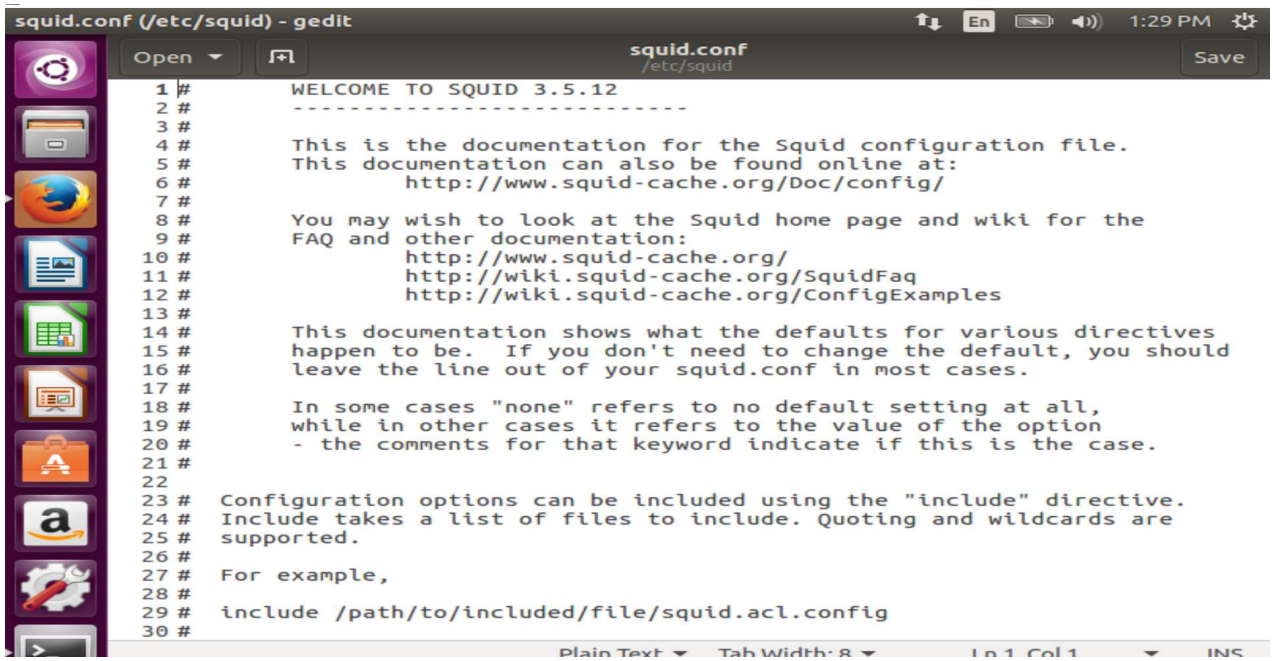
1. Go to the Edit menu and choose the Preferences option.
2. Click on Advanced, then on the Network tab, and finally on Settings.
3. Check Manual proxy configuration and enter the IP address of the proxy server and the port where it is listening for connections. Click on OK to apply changes.



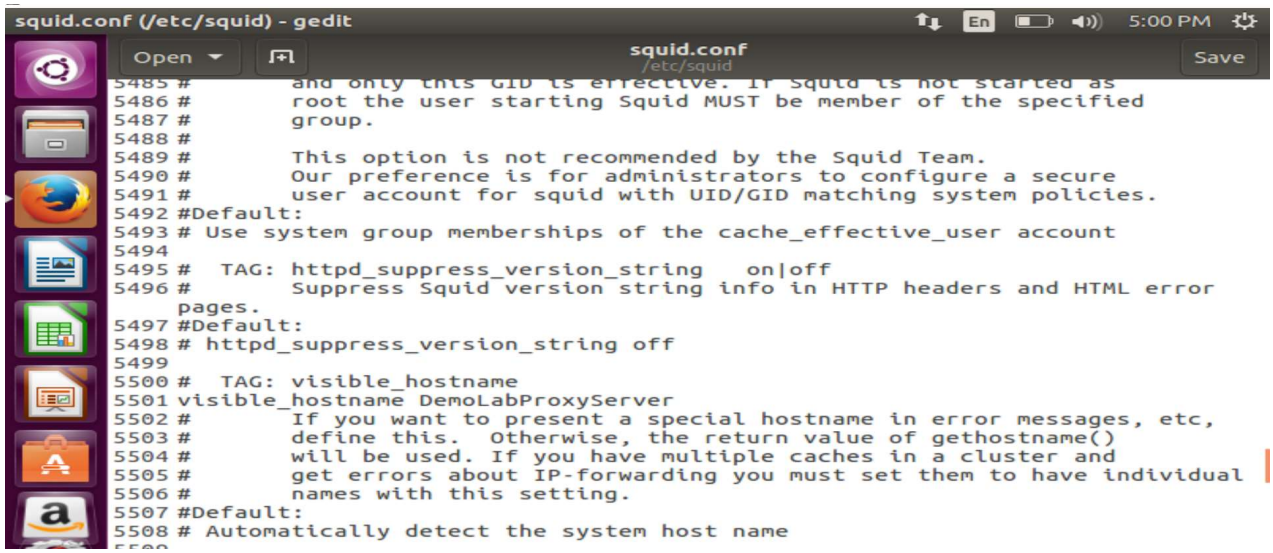
Backing up the Squid configuration file:

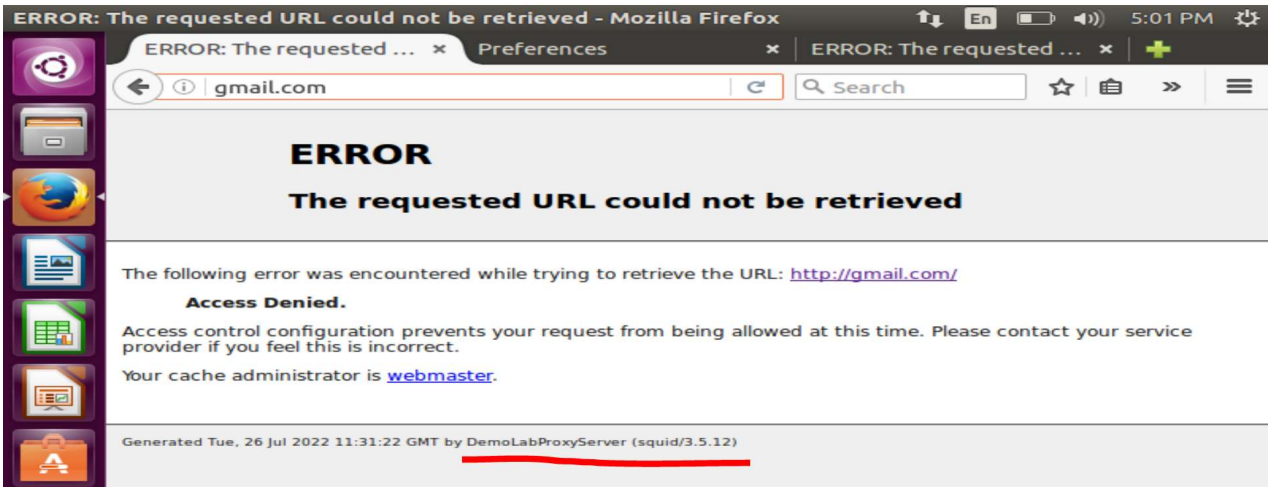
```
apeksha@apeksha-VirtualBox:/etc/squid$ cp /etc/squid/squid.conf squid.conf.copy
cp: cannot create regular file 'squid.conf.copy': Permission denied
apeksha@apeksha-VirtualBox:/etc/squid$ sudo cp /etc/squid/squid.conf squid.conf.
copy
apeksha@apeksha-VirtualBox:/etc/squid$ ls
errorpage.css  squid.conf  squid.conf.bak  squid.conf.copy
apeksha@apeksha-VirtualBox:/etc/squid$
```

SQUID Configuration file:



Change in visible proxy name:





root@apsit-HP-245-G4-Notebook-PC:~$ mv /etc/squid/squid.conf /etc/squid/squid.conf.bkp root@apsit-HP-245-G4-Notebook-PC:~$ grep -ve ^# -ve ^$ /etc/squid/squid.conf.bkp > /etc/squid/squid.conf

Now, open the newly created squid.conf file, and look for (or add) the following ACL elements and access lists.

acl localhost src 127.0.0.1/32

acl localnet src 192.168.0.40/24 192.168.0.0./16

The two lines above represent a basic example of the usage of ACL elements.

1. **The first word, acl, indicates that this is a ACL element directive line.**

2. The second word, localhost or localnet, specify a name for the directive.
3. The third word, src in this case, is an ACL element type that is used to represent a client IP address or range of addresses, respectively. Administrator can specify a single host by IP (or hostname, if you have some sort of DNS resolution implemented) or by network address.
4. The fourth parameter is a filtering argument that is "fed" to the directive.

The two lines below are access list rules and represent an explicit implementation of the ACL directives mentioned earlier. In few words, they indicate that http access should be granted if the request comes from the local network (localnet), or from localhost.

```
http_access allow localnet
http_access allow localnet
```

Squid ACL Allow Access List

At this point restart Squid in order to apply any pending changes .and then configure a client browser in the local network (192.168.3.140 in our case) to access the Internet through your proxy as follows

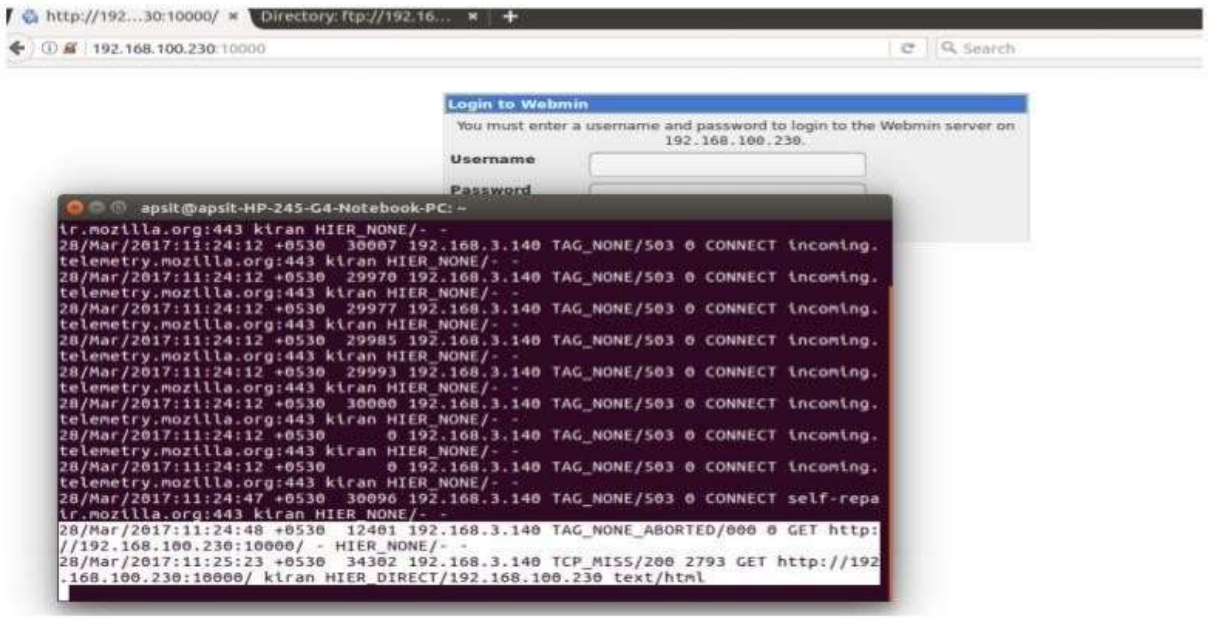
Firefox Proxy settings

4. **Go to the Edit menu and choose the Preferences option.**
5. **Click on Advanced, then on the Network tab, and finally on Settings.**
6. **Check Manual proxy configuration and enter the IP address of the proxy server and the port where it is listening for connections. Click on OK to apply changes.**

Verifying that a Client is Accessing the Internet

1. **In your client, use a web browser to open any web site .**
2. **In the server, run following command line to view of requests being served through Squid.**

root@apsit-HP-245-G4-Notebook-PC:/etc/squid$ sudo tail -f /var/log/squid/access.log


http://192...30:10000/
Directory: ftp://192.16...
192.168.100.230:10000
Search
Login to Webmin
You must enter a username and password to login to the Webmin server on 192.168.100.230.
Username
Password
apsit@apsit-HP-245-G4-Notebook-PC: ~
tr.mozilla.org:443 kiran HIER_NONE/- -
28/Mar/2017:11:24:12 +0530 30007 192.168.3.140 TAG_NONE/503 0 CONNECT incoming.
telemetry.mozilla.org:443 kiran HIER_NONE/- -
28/Mar/2017:11:24:12 +0530 29970 192.168.3.140 TAG_NONE/503 0 CONNECT incoming.
telemetry.mozilla.org:443 kiran HIER_NONE/- -
28/Mar/2017:11:24:12 +0530 29977 192.168.3.140 TAG_NONE/503 0 CONNECT incoming.
telemetry.mozilla.org:443 kiran HIER_NONE/- -
28/Mar/2017:11:24:12 +0530 29985 192.168.3.140 TAG_NONE/503 0 CONNECT incoming.
telemetry.mozilla.org:443 kiran HIER_NONE/- -
28/Mar/2017:11:24:12 +0530 29993 192.168.3.140 TAG_NONE/503 0 CONNECT incoming.
telemetry.mozilla.org:443 kiran HIER_NONE/- -
28/Mar/2017:11:24:12 +0530 30000 192.168.3.140 TAG_NONE/503 0 CONNECT incoming.
telemetry.mozilla.org:443 kiran HIER_NONE/- -
28/Mar/2017:11:24:12 +0530 0 192.168.3.140 TAG_NONE/503 0 CONNECT incoming.
telemetry.mozilla.org:443 kiran HIER_NONE/- -
28/Mar/2017:11:24:12 +0530 0 192.168.3.140 TAG_NONE/503 0 CONNECT incoming.
telemetry.mozilla.org:443 kiran HIER_NONE/- -
28/Mar/2017:11:24:47 +0530 30096 192.168.3.140 TAG_NONE/503 0 CONNECT self-repa
tr.mozilla.org:443 kiran HIER_NONE/- -
28/Mar/2017:11:24:48 +0530 12401 192.168.3.140 TAG_NONE_ABORTED/000 0 GET http:
//192.168.100.230:10000/ - HIER_NONE/- -
28/Mar/2017:11:25:23 +0530 34302 192.168.3.140 TCP_MISS/200 2793 GET http://192
.168.100.230:10000/ kiran HIER_DIRECT/192.168.100.230 text/html

Restricting Access By Client

To deny access to that particular client IP address, while yet maintaining access for the rest of the local network.

1. **Define a new ACL directive as follows**

```
acl resclient src 192.168.0.104
```

2. Add the ACL directive to the localnet access list that is already in place, but prefacing it with an exclamation sign. This means, "Allow Internet access to clients matching the localnet ACL directive except to the one that matches the resclient directive".

```
http_access allow localnet !resclient
```

3. Now restart Squid in order to apply changes. Then if client try to browse to any site we will find that access is denied now.

Restricting access by domain and / or by time of day / day of week

To restrict access to Squid by domain dstdomain keyword can be used in a ACL directive, as follows.Where forbidden_domains is a plain text file that contains the domains to deny access to.

```
acl forbidden dstdomain "/etc/squid/forbidden_domains"
```

root@apsit-HP-245-G4-Notebook-PC:/etc/squid$ cat forbidden_domains

.facebook.com

localhost

To grant access to Squid for requests not matching the directive above.

http_access allow localnet ! forbidden

To allow access to those sites during a certain time of the day (10:00 until 11:00 am) only on Monday (M), Wednesday (W), and Friday (F).

```
acl workingHour time MWFA 10:00-11:00
http_access allow forbidden workingHour
http_access deny forbidden
```

Restricting access by user authentication

Squid support several authentication mechanisms. To use Basic authentication withNCSA. Add the following lines to your /etc/squid/squid.conf file.

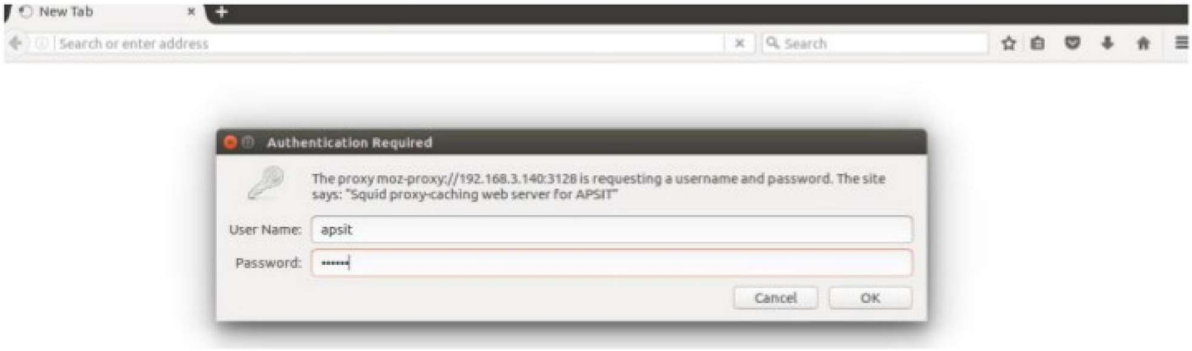
```
auth_param basic program /usr/lib/squid3/basic_ncsa_auth
/etc/squid/passwd
auth_param basic credentialsttl 30 minutes
auth_param basic casesensitive on
auth_param basic realm Squid proxy-caching web server for APSIT
acl ncsa proxy_auth REQUIRED
http_access allow ncsa
```

Details of acl and acl directives used:

1. To tell Squid which authentication helper program to use with the auth_param directive by specifying the name of the program plus any command line options (/etc/squid/passwd in this case) if necessary.
2. The /etc/squid/passwd file is created through htpasswd, a tool to manage basic authentication through files. It will allow us to add a list of usernames (and their corresponding passwords) that will be allowed to use Squid.
3. Credentialsttl 30 minutes will require entering your username and password every 30 minutes
4. Casesensitive on indicates that usernames and passwords are case sensitive.
5. Realm represents the text of the authentication dialog that will be used to authenticate to squid.
6. Finally, access is granted only when proxy authentication (proxy_auth REQUIRED) succeeds.

Run the following command to create the file and to add credentials for user apsit (omit the -c flag if the file already exists) and Open a web browser in the client machine and try to browse to any given site.

```
root@apsit-HP-245-G4-Notebook-PC:~# htpasswd /etc/squid/passwd apsit
New password:
Re-type new password:
Adding password for user apsit
root@apsit-HP-245-G4-Notebook-PC:~# cat /etc/squid/passwd | grep apsit
apsit:$apr1$tTA.ZAfI$O4JBblrCY1QOeFQKwv.ko/
root@apsit-HP-245-G4-Notebook-PC:~#
```



Note : By default, Squid listens on port 3128, but administrator can override this behavior by editing the access list rule that begins with http_port (by default it reads http_port 3128). Also after any updation squid daemon has to be restarted to make changes permanent.

Conclusion: Conclusion: Hence we have successfully studied how Squid Proxy server can be used for providing security controls for web servers & protecting servers from unauthorised access by using Access Control Lists(ACLs). As well as we have studied how squid can be used to filter traffic on HTTP, FTP, and HTTPS, and increase the speed (thus lower the response time) for a web server via caching