



PARSHVANATH CHARITABLE TRUST'S

**A. P. SHAH INSTITUTE OF TECHNOLOGY**

(All Branches NBA Accredited)



---

## 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 original site. 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



PARSHVANATH CHARITABLE TRUST'S

# A. P. SHAH INSTITUTE OF TECHNOLOGY

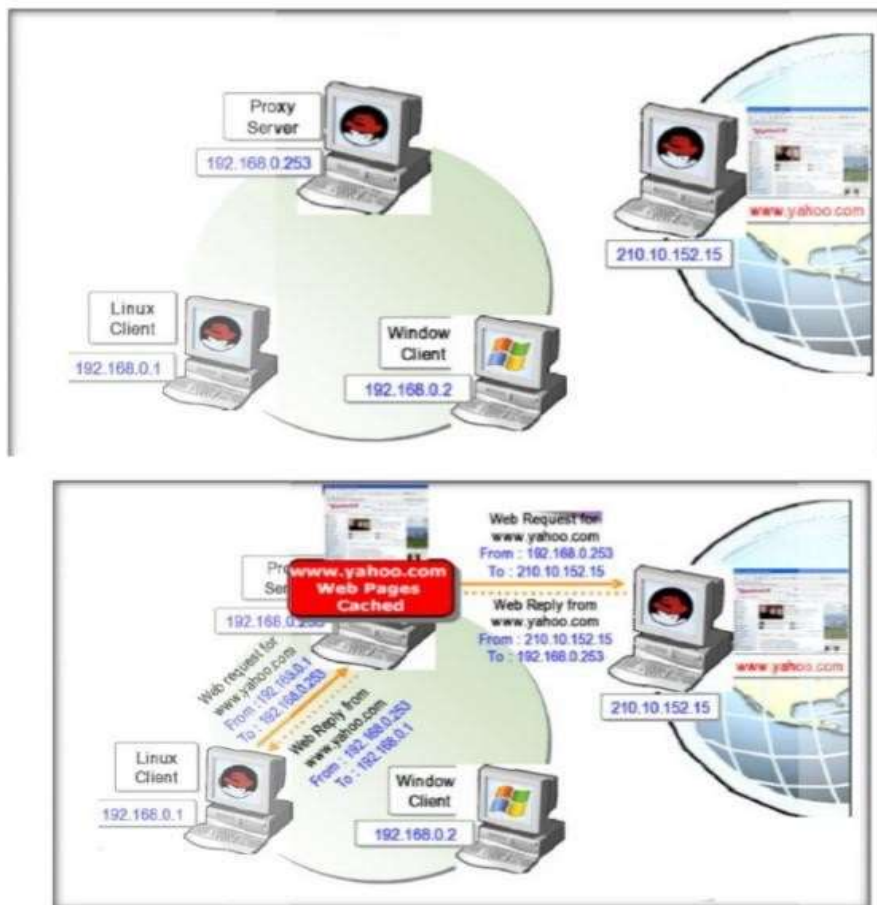
(All Branches NBA Accredited)



client1 downloads 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`

```
apeksha@apeksha-VirtualBox: ~  
apeksha@apeksha-VirtualBox:~$ lsb_release -a  
No LSB modules are available.  
Distributor ID: Ubuntu  
Description:    Ubuntu 16.04 LTS  
Release:        16.04  
Codename:       xenial  
apeksha@apeksha-VirtualBox:~$ sudo apt-get install squid  
[sudo] password for apeksha:  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
squid is already the newest version (3.5.12-1ubuntu7.16).  
0 upgraded, 0 newly installed, 0 to remove and 759 not upgraded.  
apeksha@apeksha-VirtualBox:~$
```



## Check status of SQUID :

```
apeksha@apeksha-VirtualBox: /etc/squid
apeksha@apeksha-VirtualBox:~$ cd /etc/squid/
apeksha@apeksha-VirtualBox:/etc/squid$ ls
errorpage.css  squid.conf  squid.conf.bak
apeksha@apeksha-VirtualBox:/etc/squid$ sudo /etc/init.d/squid status
● squid.service - LSB: Squid HTTP Proxy version 3.x
   Loaded: loaded (/etc/init.d/squid; bad; vendor preset: enabled)
   Active: active (running) since Tue 2022-07-26 13:21:07 IST; 3min 26s ago
     Docs: man:systemd-sysv-generator(8)
  Process: 1130 ExecStart=/etc/init.d/squid start (code=exited, status=0/SUCCESS)
    Tasks: 4 (limit: 512)
   CGroup: /system.slice/squid.service
           └─1177 /usr/sbin/squid -YC -f /etc/squid/squid.conf
             └─1182 (squid-1) -YC -f /etc/squid/squid.conf
               └─1185 (logfile-daemon) /var/log/squid/access.log
                 └─1186 (pinger)

Jul 26 13:21:07 apeksha-VirtualBox systemd[1]: Starting LSB: Squid HTTP Proxy ve
Jul 26 13:21:07 apeksha-VirtualBox squid[1130]: * Starting Squid HTTP Proxy squ
Jul 26 13:21:07 apeksha-VirtualBox squid[1130]: ...done.
Jul 26 13:21:07 apeksha-VirtualBox systemd[1]: Started LSB: Squid HTTP Proxy ver
Jul 26 13:21:07 apeksha-VirtualBox squid[1177]: Squid Parent: will start 1 kids
Jul 26 13:21:07 apeksha-VirtualBox squid[1177]: Squid Parent: (squid-1) process
lines 1-18/18 (END)
```

## 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.





PARSHVANATH CHARITABLE TRUST'S

**A. P. SHAH INSTITUTE OF TECHNOLOGY**

(All Branches NBA Accredited)



**Connection Settings**

**Configure Proxies to Access the Internet**

☐ No proxy

☐ Auto-detect proxy settings for this network

☐ Use system proxy settings

☒ **Manual proxy configuration:**

HTTP Proxy:  Port:

☐ Use this proxy server for all protocols

SSL Proxy:  Port:

FTP Proxy:  Port:

SOCKS Host:  Port:

☐ SOCKS v4 ☒ SOCKS v5 ☐ Remote DNS

No Proxy for:

Example: .mozilla.org, .net.nz, 192.168.1.0/24

☐ Automatic proxy configuration URL:

☐ Do not prompt for authentication if password is saved

**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:**



PARSHVANATH CHARITABLE TRUST'S

# A. P. SHAH INSTITUTE OF TECHNOLOGY

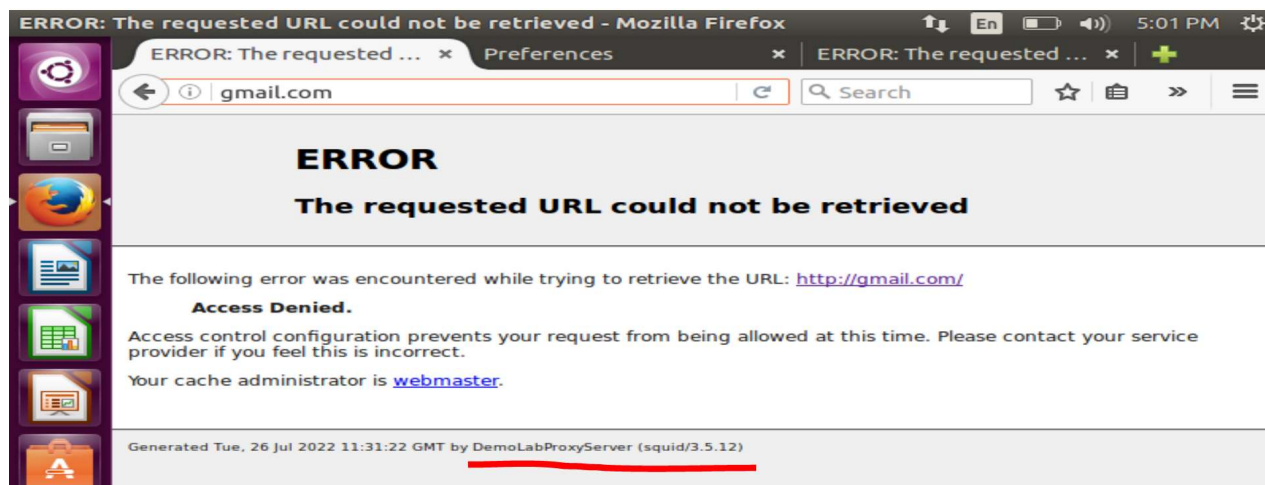
(All Branches NBA Accredited)



```
squid.conf (/etc/squid) - gedit
1 # WELCOME TO SQUID 3.5.12
2 # -----
3 #
4 # This is the documentation for the Squid configuration file.
5 # This documentation can also be found online at:
6 # http://www.squid-cache.org/Doc/config/
7 #
8 # You may wish to look at the Squid home page and wiki for the
9 # FAQ and other documentation:
10 # http://www.squid-cache.org/
11 # http://wiki.squid-cache.org/SquidFaq
12 # http://wiki.squid-cache.org/ConfigExamples
13 #
14 # This documentation shows what the defaults for various directives
15 # happen to be. If you don't need to change the default, you should
16 # leave the line out of your squid.conf in most cases.
17 #
18 # In some cases "none" refers to no default setting at all,
19 # while in other cases it refers to the value of the option
20 # - the comments for that keyword indicate if this is the case.
21 #
22 # Configuration options can be included using the "include" directive.
23 # Include takes a list of files to include. Quoting and wildcards are
24 # supported.
25 #
26 # For example,
27 #
28 # include /path/to/included/file/squid.acl.config
29 #
30 #
```

## Change in visible proxy name:

```
squid.conf (/etc/squid) - gedit
5485 # and only this GID is effective. If Squid is not started as
5486 # root the user starting Squid MUST be member of the specified
5487 # group.
5488 #
5489 # This option is not recommended by the Squid Team.
5490 # Our preference is for administrators to configure a secure
5491 # user account for squid with UID/GID matching system policies.
5492 #Default:
5493 # Use system group memberships of the cache_effective_user account
5494 #
5495 # TAG: httpd_suppress_version_string on/off
5496 # Suppress Squid version string info in HTTP headers and HTML error
5497 # pages.
5498 #Default:
5499 # httpd_suppress_version_string off
5500 # TAG: visible_hostname
5501 visible_hostname DemoLabProxyServer
5502 # If you want to present a special hostname in error messages, etc,
5503 # define this. Otherwise, the return value of gethostname()
5504 # will be used. If you have multiple caches in a cluster and
5505 # get errors about IP-forwarding you must set them to have individual
5506 # names with this setting.
5507 #Default:
5508 # Automatically detect the system host name
5509 #
```



```
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.



PARSHVANATH CHARITABLE TRUST'S

## A. P. SHAH INSTITUTE OF TECHNOLOGY

(All Branches NBA Accredited)



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 localhost
```

```
http_access allow localnet
```







PARSHVANATH CHARITABLE TRUST'S

## A. P. SHAH INSTITUTE OF TECHNOLOGY

(All Branches NBA Accredited)



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.

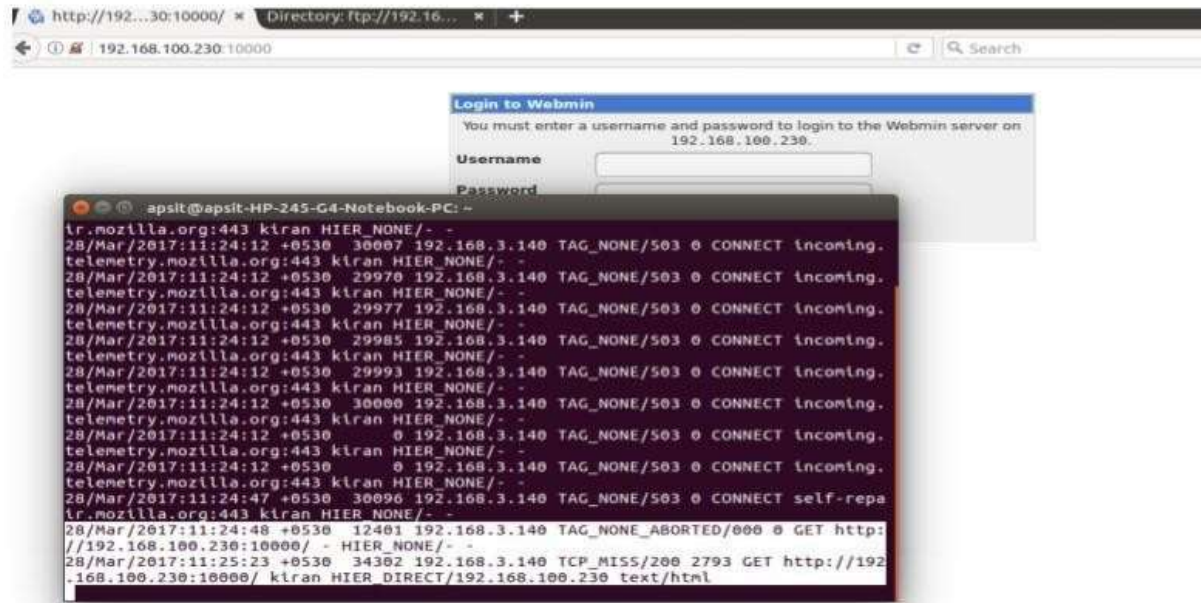
### Verifying that a Client is Accessing the Internet

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
```



PARSHVANATH CHARITABLE TRUST'S  
**A. P. SHAH INSTITUTE OF TECHNOLOGY**  
(All Branches NBA Accredited)





PARSHVANATH CHARITABLE TRUST'S

**A. P. SHAH INSTITUTE OF TECHNOLOGY**

(All Branches NBA Accredited)



## 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"
```



PARSHVANATH CHARITABLE TRUST'S

**A. P. SHAH INSTITUTE OF TECHNOLOGY**

(All Branches NBA Accredited)



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 with NCSA.

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`





PARSHVANATH CHARITABLE TRUST'S

**A. P. SHAH INSTITUTE OF TECHNOLOGY**

**(All Branches NBA Accredited)**



#### **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.



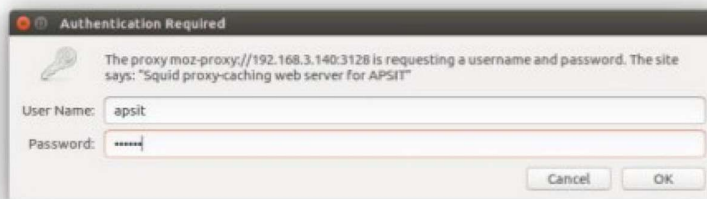
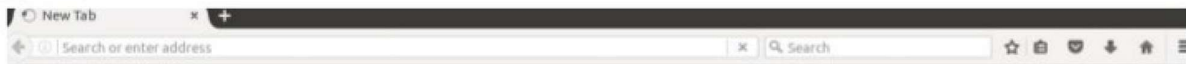
PARSHVANATH CHARITABLE TRUST'S

# A. P. SHAH INSTITUTE OF TECHNOLOGY

(All Branches NBA Accredited)



```
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.ZAfISD4JBblrCY1Q0eFQKwv.ko/
root@apsit-HP-245-G4-Notebook-PC:~#
```





PARSHVANATH CHARITABLE TRUST'S  
**A. P. SHAH INSTITUTE OF TECHNOLOGY**  
(All Branches NBA Accredited)



**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