Academic Year: 2023-24 **Semester: V**
Class / Branch: TE IT
Subject: Security Lab (SL)
Subject Lab Incharge: Prof. Apeksha Mohite

EXPERIMENT NO. 2

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

Theory:

Squid is a free, open source, proxy-caching server for web clients, designed to speedInternet 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 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 anetwork 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).

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"

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**

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 viacaching.