**Squid Proxy Server Interview Questions & Answers**

**Q:1 What is Proxy Server and why it is used ?**

Ans: A proxy server provides Internet access to different users at same time i.e by sharing a single Internet connection. A good proxy server also provides for caching of the requests, which helps to access data from local resources rather fetching the data from web thus reducing access time and bandwidth.

**Q:2 What is Squid and its features ?**

Ans: Squid is proxy server for UNIX like operating system, A Squid proxy server filters Web traffic and caches frequently accessed files. A proxy server limits Internet bandwidth usage, speeds up Web access, and lets you filter URLs. Centrally blocking advertisements and dangerous downloads is cost effective and transparent for the end user. Squid is a high per-formance implementation of a free Open-Source, full-featured proxy caching server.

**Q:3 What is the default configuration file of Squid ?**

Ans: ‘/etc/squid/squid.conf‘ is the default configuration file of Squid.

**Q:4 What is the default port of Squid and how to change it ?**

Ans: Default port of squid is 3128 and we can change the default port by the editing the file /etc/squid/squid.conf :

http\_port 3128

Change this port according to your setup. After editing the file one should restart the squid service.

**Q:5 How to restart the squid service in CentOS  & RHEL ?**

Ans: Service squid restart or /etc/init.d/squid restart

**Q:6 What are the different filters that we can apply using squid ?**

Ans: Some of the filters are listed below :

* domains of client or server
* IP subnets of client or server
* URL path
* Full URL including parameters
* keywords
* ports
* protocols: HTTP, FTP
* methods: GET, POST, HEAD, CONNECT

**Q:7 What is ACL in Squid ?**

Ans: ACL stands for **Access Control List** , using ACL access to internet can be controlled  in terms of access during particular time interval, caching, access to particular or group of sites, etc.Squid access control has two different components i.e. ACL elements and access list. An access list infact allows or deny the access to the service.

**Q:8 What are the important ACL elements in Squid ?**

Ans: A few important type of ACL elements are listed below

* src : Source i.e. client’s IP addresses
* dst : Destination i.e. server’s IP addresses
* srcdomain : Source i.e. client’s domain name
* dstdomain : Destination i.e. server’s domain name
* time : Time of day and day of week
* url\_regex : URL regular expression pattern matching
* urlpath\_regex: URL-path regular expression pattern matching, leaves out the protocol and hostname
* proxy\_auth : User authentication through external processes
* maxconn : Maximum number of connections limit from a single client IP address

To apply the controls, one has to first define set of ACL and then apply rules on them. The format of an ACL statement is

acl acl\_element\_name type\_of\_acl\_element values\_to\_acl

**Q:9 Write a rule allowing only selected machines to have access to the Internet ?**

Ans: Edit the config file /etc/squid/squid.conf :

acl allowed\_clients src 192.168.1.10 192.168.1.20 192.168.1.30

http\_access allow allowed\_clients

http\_access deny !allowed\_clients

Above rule will allow only machine whose IPs are 192.168.1.10,192.168.1.20 & 192.168.1.30 to have access to Internet and the rest of IP addresses (not listed ) are denied the service. After editing the file don’t forget to restart the squid service.

**Q:10 Allow Internet access during particular period of time ?**

Ans: Edit the file ‘/etc/squid/squid.conf’ and add the below rules :

acl allowed\_clients src 192.168.1.1/255.255.255.0

acl regular\_days time MTWHF 10:00-16:00

http\_access allow allowed\_clients regular\_days

http\_access deny allowed\_clients

This will allow the access to all the clients in network 192.168.1.1 to access the net from Monday to Friday from 10:00am to 4:00 pm.

**Q:11 How to enable multiple time Internet access to different clients in squid ?**

Ans:  Edit the config file and add below rules :

acl hosts1 src192.168.1.10

acl hosts2 src 192.168.1.20

acl hosts3 src 192.168.1.30

acl morning time 10:00-13:00

acl lunch time 13:30-14:30

acl evening time 15:00-18:00

http\_access allow host1 morning

http\_access allow host1 evening

http\_access allow host2 lunch

http\_access allow host3 evening

http\_access deny all

The above rule will allow host1 access during both morning as well as evening hours; where as host2 and host3 will be allowed access only during lunch and evening hours respectively.

**Q:12 How to block websites using squid ?**

Ans: Squid can prevent the access to a particular site or to sites which contain a particular word. This can be implemented by adding the below rules in the ‘/etc/squid/squid.conf’ file.

acl allowed\_clients src 192.168.1.1/255.255.255.0

acl banned\_sites url\_regex "/etc/banned.list"

http\_access deny banned\_sites

http\_access allow allowed\_clients

Create a file /etc/banned.list , add all the sites that you want to block.

**Q:13 How to limit the number of connections from a client machine in squid ?**

Ans: Squid can limit number the of connections from the client machine and this is possible through the maxconn element. To use this option, client\_db feature should be enabled first.

acl mynetwork 192.168.1.1/255.255.255.0

acl numconn maxconn 5

http\_access deny mynetwork numconn

maxconn ACL uses less-than comparison. This ACL is matched when the number of connections is greater than the specified value. This is the main reason for which this ACL is not used with the http\_access allow rule.

**Q:14 What is reverse proxy ?**

Ans: A reverse proxy is a type of proxy server or ‘webserver acceleration’ (using http\_port 80 accel vhost) , in this type of proxy server , the cache serves an unlimited number of clients for a limited number of or just one web server.

**Q:15 What is transparent proxy ?**

Ans:  Transparent proxy is a type of proxy server where clients are not aware that their requests are processed through the proxy. The main benefit of setting transparent proxy is that  system admins do not have to setup up individual browsers to work with proxies, squid will transparently pick up the appropriate packets and cache requests.

**Q:16 How to clear Squid Cache ?**

Ans: To clear the squid cache , first stop the squid service and run below command :

# service squid stop

# rm -rf /var/lib/squid/cache/\*

Now create swap directories :

# squid –z

**Q:17 How to check live running logs of squid  ?**

Ans: To see the live logs of squid use the below command :