**How to Block Websites in Squid Proxy (centos\_7)**

**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.**

**Most of the Linux system admins want to install squid to give restricted internet access to their clients computers. In this short tutorial will look, how to block websites in squid proxy using ACL (Access Control List).**

**Installing Squid on CentOS**

**Squid package is included in the default CentOS 7 repositories. To install it run**

yum install squid -y

**Once the installation is completed, start and enable the Squid service:**

sudo systemctl start squid

sudo systemctl enable squid

**We have couple of ways to block specific domain name in squid proxy server.**

**1) Block specif domain by creating ban list of bad websites.**

**2) Block specifying the domain name directly in the squid config file.**

**Create a file called ban\_domains and then specify the path of this file in ACL to block websites in squid proxy.**

**Create file using vi editor**

vi /etc/squid/ban\_domains.txt

**Add ban domains name line by line**

www.yahoo.com

www.gmail.com

www.youtube.com

www.facebook.com

**save and exit.**

**Now add ACL to filter ulrs by checking our ban list and then deny access with http\_access see below:**

**Edit squid configuration file**

# vi /etc/squid/squid.conf

Add these lines in ACL Section (below the ACL ports)

acl ban\_domains dstdomain "/etc/squid/ban\_domains.txt"

http\_access deny ban\_domains

**save and exit**

**Restart squid service to apply changes**

service squid restart

**if you dont want to make directory to block websites list then you can directly add the website domain in /etc/squid/squid.conf**

**You will get the same result by doing the following changes in squid.conf.**

vi /etc/squid/squid.conf

acl ban\_domains dstdomain .gmail.com.com .oyo.com .zoomcar.com

http\_access deny ban\_domains

service squid restart

**Note:- If you follow this Document correctly and still not able to block YouTube.com and Facebook.com, so you might be trying to block “HTTPS domains” e.g (https://youtube.com or https://facebook.com) using this method. This method will not work for HTTPS domains**

**On Client Machine (Windows)**

**Now open up chrome browser on client computer and point squid server IP in proxy settings with 3128 port.**

Click the **Triple dot** button and then **select Settings.**

you see the "**advanced**" link and then click on it**.**

then click on **"Accessibility"**

you can see **"Open proxy settings"**

On the Internet Properties window**,** click on the **"LAN settings"** button**.**

In the LAN Settings, uncheck the box that says **"Automatically detect settings."** And then, in the Proxy Server section, click the checkbox to enable **"Use a proxy server for your LAN..."**

In the Address field, enter the IP Address of your Proxy Server, and the Proxy Server Port Number in the Port field.

**Press the OK button and then press OK again to save your settings.**

**then type the URL in search bar yahoo.com**

you will see this type of error

