**How to Install and Configure Squid Proxy on 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.

Squid Proxy is an open source caching proxy for the web. It supports many protocols such as HTTP, HTTPS, FTP and more. It improves the response time and reduces bandwidth by caching and reusing the frequently accessed web pages and files. In this tutorial we will learn to install Squid Proxy on CentOS 7. We will also learn about some basic configuration which can be done on Squid caching server.

**HTTP**

HTTP means HyperText Transfer Protocol. HTTP is the underlying protocol used by the World Wide Web and this protocol defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands.

**HTTPS**

Hyper Text Transfer Protocol Secure (HTTPS) is the secure version of HTTP, the protocol over which data is sent between your browser and the website that you are connected to. The 'S' at the end of HTTPS stands for 'Secure'. It means all communications between your browser and the website are encrypted.

**Requirements**

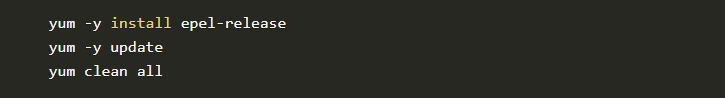
Squid does not have any minimum hardware requirements, but the amount of RAM may vary according to the users accessing the Internet through your proxy and the objects stored in the cache. To follow this tutorial you will need a CentOS 7.x server with root access on it. If you are logged in as non root user, run sudo -i to switch to root user. You can also use sudo command before all the administrative commands to run them as root user.

**Installing Squid**

Before installing any packages, it is recommended to update the system and packages using the following command.

1.PNG

Now you will need to install EPEL repository to your system as Squid is not available in default yum repository. Run the following command to install EPEL repository in your server.



Now you can install Squid Proxy using the following command.

3.PNG

Once you install Squid, you can start the program immediately using the following command.

4.PNG

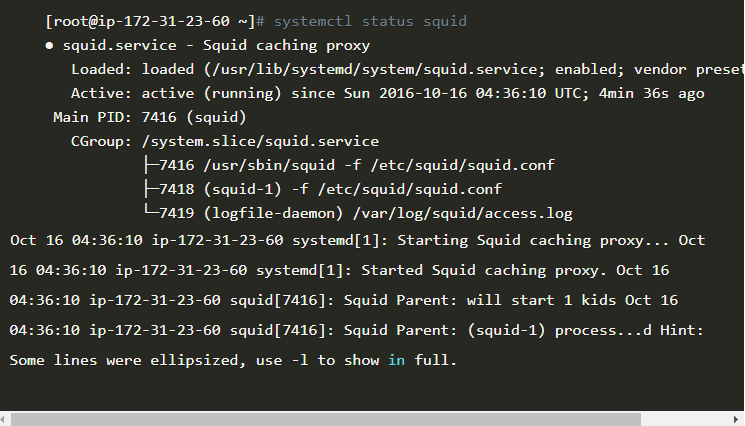
To automatically start Squid at boot time you can run the following command.

5.PNG

To view the status of Squid service, run the following command.

6.PNG

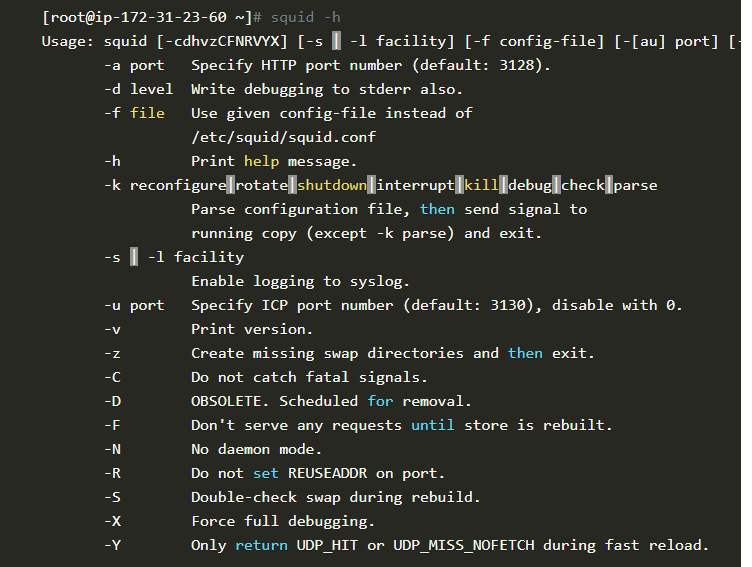
You will see an output similar to this.



To view the available options with squid command, run the following command.

8.PNG

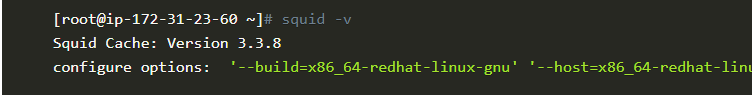
You will see output similar to this.



To view the Squid version and configuration options, run the following command

10.PNG

You will likely see the following output.



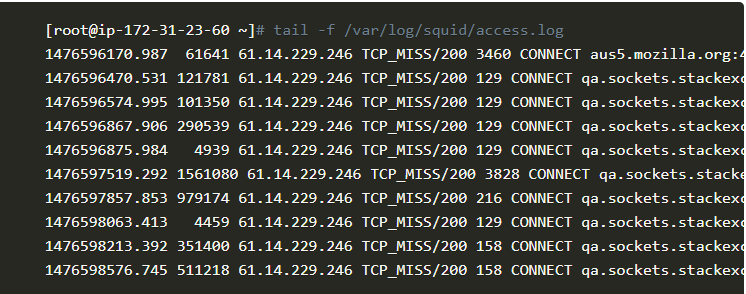
The main configuration file for Squid proxy can be found on /etc/squid/squid.conf. You can now setup your browser to use the proxy server you just created. For Internet Explorer and Google Chrome, you can go to Control Panel > Internet Options. In the Connections tab, click on LAN settings and enter your proxy server IP address and port 3128. You will see that you are now browsing the internet through the proxy server.

By default the Squid proxy server is configured to connect to a local network only, if you are not into the local network of the proxy server, you will see an error saying *"The proxy server is refusing connections"*. If you are getting these kind of errors, then you will need to configure Access Control Lists or ACL into the squid configuration file.

You can check the error logs of Squid using the following command.

12.PNG

You will see an output similar to shown below.



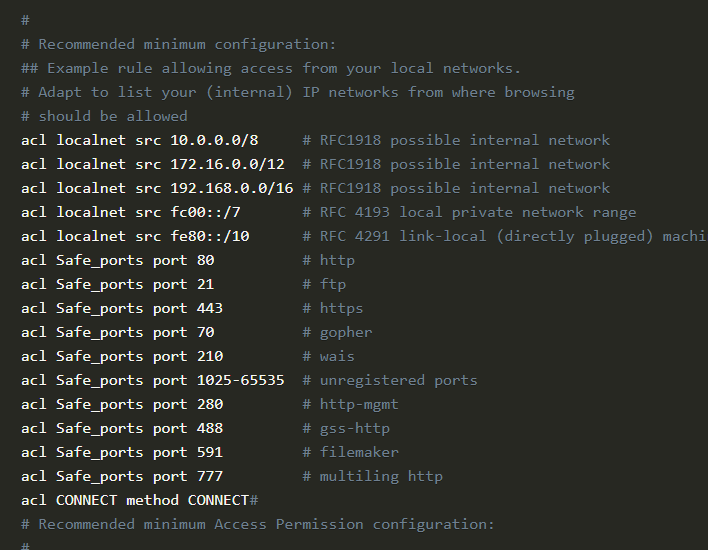
**Configuring Squid**

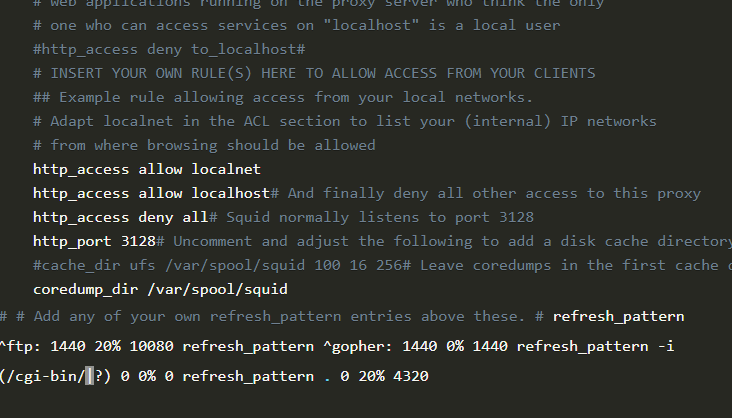
Squid can be easily configured by editing the global configuration file /etc/squid/squid.conf. To edit the configuration file run the following command.

1.PNG

You can use any editor of your choice, in this tutorial we will be using nano editor. If you don't have nano editor installed, you can run yum -y install nano command to install nano editor.

A minimum sample configuration file will look like this.



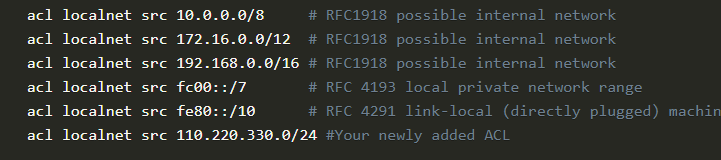


**Allow IP Address to Use the Internet Through Your Proxy Server**

To allow a range of IP address to use the Internet through your proxy server. You can add a new ACL entry. Squid supports CIDR notations. Consider an example, if you want to allow a range of IP address from 110.220.330.1 to 110.220.330.255 then you can make the following entry in Squid configuration file under the list of ACLs.

4.PNG

Your list of ACLs will finally look like this

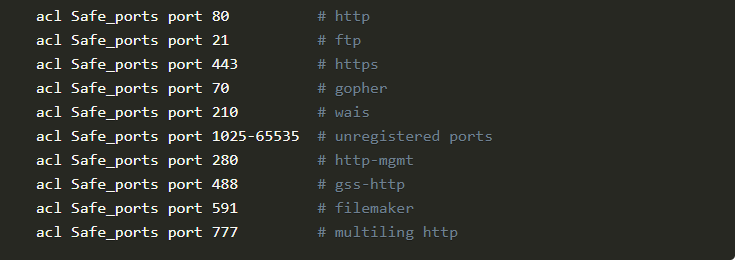


For changes to take effect you will need to restart your Squid server, use the following command for same.

6.PNG

**Allow a Specific Port for HTTP Connections**

By default Squid only consider very few ports as safe ports and allow connections through them. The ports which are allowed by default are:



The ports which are not listed above will not be accessed through the proxy. You can add a Port into the list of Safe\_ports by modifying the list of ACLs for ports. For example it you want to allow port 168 to be accessed through the proxy server you can add the following ACL entry for this.

8.PNG

For changes to take effect you will need to restart your Squid server, use the following command for same.

9.PNG

**Using Basic Authentication with Squid**

If you want to authenticate the user before they can use your proxy server, you can do it using the basic authentication feature available in Squid proxy. Although Squid supports many kind of authentication but basic authentication is very easy to set up.

First of all you will need to install httpd-tools, which comes with a tool htpasswd which we will use to create an encrypted password file. Run the following command to install httpd-tools.

10.PNG

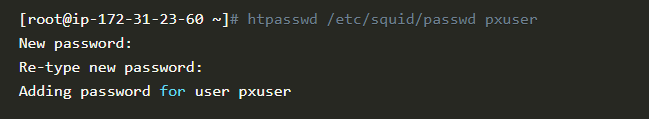
Now create a new file and provide the ownership to squid daemon so that it can access it. Run the following command for same.

11.PNG

Now you can add a new user to the password file using the htpasswd tool. In this tutorial we will be creating an example user pxuser. You can replace pxuser with anything you like. Run the following command to create a new user using  htpasswd tool.

12.PNG

It will ask for the new password twice, provide the password and you will see following output.

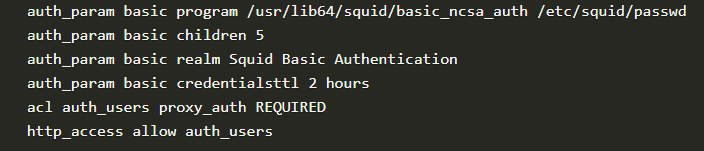


By default htpasswd uses MD5 encryption for the password, hence your password will be stored in MD5 hash.

As we have our password file ready, you can now edit the squid configuration file using the following command.

14.PNG

Add the following lines into the configuration file under the access control lists of ports.



Write the changes to the file and exit from editor. Reload the Squid daemon using the following command.

.1.PNG

Now if you will try to use the proxy server, it will ask you for authentication. Provide your username and password and you will be able to use the proxy server. Unauthenticated user will be shown an error page.

8.PNG

**Blocking Websites**

You can easily block a single or a list of websites from the users. Using a separate file for the list of websites to be blocked is a good way to manage the blocked websites. Create a new file to store the list of websites to be blocked using your favorite editor.

2.PNG

Now enter the list of sites you want to block. One website per line.



Save the file and exit the editor. In this example we used some example websites, you can put a list of actual websites you wish to block. Now open the Squid configuration file again using the following command.

4.PNG

Enter the following lines under acl list and http\_access list.

5.PNG

Write the changes to the file and exit from editor. Reload the Squid daemon using the following command.

6.PNG

Now if you will try to access the blocked sites, you will get an *access denied* message from Squid.

**Changing Squid Port**

You can easily change the port on which squid listens to. Edit the configuration file using the following command.

7.PNG

Scroll down to find the following lines into the file.

8.PNG

Now change the http\_port from 3128 to any port you want. Make sure that no other service is using the port which you will use for Squid. Now restart the Squid daemon and you will see that the changes are in effect.

**Conclusion**

In this detailed tutorial we learned how to install Squid proxy server on CentOS 7 systems. You can now easily setup a basic installation of Squid. You also learnt about some basic configuration of Squid proxy server inclusding enabling basic authentication.