Assignments:11

Module:- COSA(Proxy Server and squid proxy)
Name:- Prithviraj Nikam

Lab Assignment :-

What is proxy?

As the need for internet access at the workplace grows, web proxies come from a need to secure an organization's internal network from external threats. Broadly speaking, a web proxy, also referred to as a proxy or proxy server, is a way to filter the connection between your computer and the internet.

What is proxy server?

Proxy server is a system or router that provides a gateway between users and the internet. Therefore, it helps prevent cyber attackers from entering a private network. It is a server, referred to as an "intermediary" because it goes between end-users and the web pages they visit online.

When a computer connects to the internet, it uses an IP address. This is similar to your home's street address, telling incoming data where to go and marking outgoing data with a return address for other devices to authenticate. A proxy server is essentially a computer on the internet that has an IP address of its own.

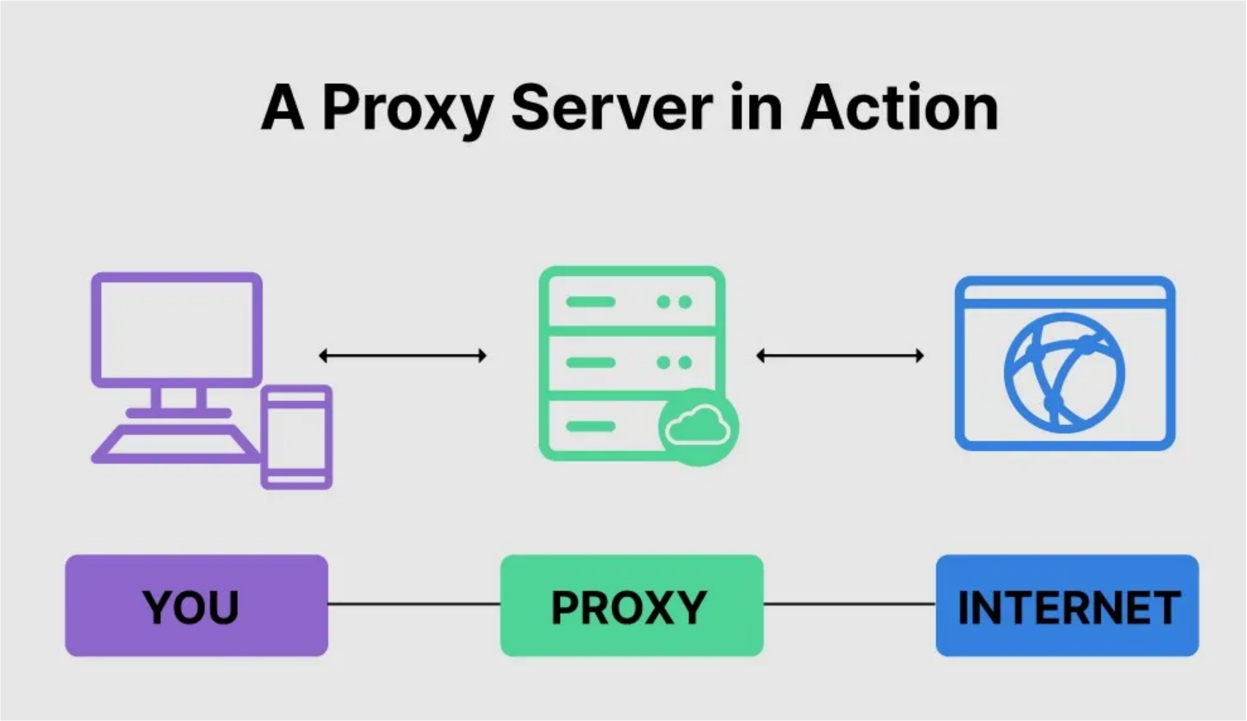
Proxy Servers and Network Security.

Proxies provide a valuable layer of security for your computer. They can be set up as web filters or firewalls, protecting your computer from internet threats like malware.

This extra security is also valuable when coupled with a secure web gateway or other email security products. This way, you can filter traffic according to its level of safety or how much traffic your network—or individual computers—can handle.

How to use a proxy? Some people use proxies for personal purposes, such as hiding their location while watching movies online, for example. For a company, however, they can be used to accomplish several key tasks such as:

1. Improve security
2. Secure employees' internet activity from people trying to snoop on them
3. Balance internet traffic to prevent crashes
4. Control the websites employees and staff access in the office
5. Save bandwidth by caching files or compressing incoming traffic



How a Proxy Works

Because a proxy server has its own IP address, it acts as a go-between for a computer and the internet. Your computer knows this address, and when you send a request on the internet, it is routed to the proxy, which then gets the response from the web server and forwards the data from the page to your computer's browser, like Chrome, Safari, Firefox, or Microsoft Edge

How to Get a Proxy

There are hardware and software versions. Hardware connections sit between your network and the internet, where they get, send, and forward data from the web. Software proxies are typically hosted by a provider or reside in the cloud. You download and install an application on your computer that facilitates interaction with the proxy.

Often, a software proxy can be obtained for a monthly fee. Sometimes, they are free. The free versions tend to offer users fewer addresses and may only cover a few devices, while the paid proxies can meet the demands of a business with many devices.

How Is the Server Set Up?

To get started with a proxy server, you have to configure it in your computer, device, or network. Each operating system has its own setup procedures, so check the steps required for your computer or network.

In most cases, however, setup means using an automatic configuration script. If you want to do it manually, there will be options to enter the IP address and the appropriate port.

How Does the Proxy Protect Computer Privacy and Data?

A proxy server performs the function of a firewall and filter. The end-user or a network administrator can choose a proxy designed to protect data and privacy. This examines the data going in and out of your computer or network. It then applies rules to prevent you from having to expose your digital address to the world. Only the proxy’s IP address is seen by hackers or other bad actors. Without your personal IP address, people on the internet do not have direct access to your personal data, schedules, apps, or files.

With it in place, web requests go to the proxy, which then reaches out and gets what you want from the internet. If the server has encryption capabilities, passwords and other personal data get an extra tier of protection.

Benefits of a Proxy Server

Proxies come with several benefits that can give your business an advantage:

1. **Enhanced security**: Can act like a firewall between your systems and the internet. Without them, hackers have easy access to your IP address, which they can use to infiltrate your computer or network.
2. **Private browsing, watching, listening, and shopping**: Use different proxies to help you avoid getting inundated with unwanted ads or the collection of IP-specific data.
3. **Access to location-specific content**: You can designate a proxy server with an address associated with another country. You can, in effect, make it look like you are in that country and gain full access to all the content computers in that country are allowed to interact with.
4. **Prevent employees from browsing inappropriate or distracting sites**: You can use it to block access to websites that run contrary to your organization's principles. Also, you can block sites that typically end up distracting employees from important tasks. Some organizations block social media sites like Facebook and others to remove time-wasting temptations.

Types of Proxy Servers

While all proxy servers give users an alternate address with which to use the internet, there are several different kinds—each with its own features.

Forward Proxy

A forward proxy sits in front of clients and is used to get data to groups of users within an internal network. When a request is sent, the proxy server examines it to decide whether it should proceed with making a connection.

A forward proxy is best suited for internal networks that need a single point of entry. It provides IP address security for those in the network and allows for straightforward administrative control. However, a forward proxy may limit an organization's ability to cater to the needs of individual end-users.

Transparent Proxy

A transparent proxy can give users an experience identical to what they would have if they were using their home computer. In that way, it is “transparent.” They can also be “forced” on users, meaning they are connected without knowing it.

Transparent proxies are well-suited for companies that want to make use of a proxy without making employees aware they are using one. It carries the advantage of providing a seamless user experience. On the other hand, transparent proxies are more susceptible to certain security threats, such as SYN-flood denial-of-service attacks.

Anonymous Proxy

An anonymous proxy focuses on making internet activity untraceable. It works by accessing the internet on behalf of the user while hiding their identity and computer information.

A transparent proxy is best suited for users who want to have full anonymity while accessing the internet. While transparent proxies provide some of the best identity protection possible, they are not without drawbacks. Many view the use of transparent proxies as underhanded, and users sometimes face pushback or discrimination as a result.

High Anonymity Proxy

A high anonymity proxy is an anonymous proxy that takes anonymity one step further. It works by erasing your information before the proxy attempts to connect to the target site.

The server is best suited for users for whom anonymity is an absolute necessity, such as employees who do not want their activity traced back to the organization. On the downside, some of them, particularly the free ones, are decoys set up to trap users in order to access their personal information or data.

Distorting Proxy

A distorting proxy identifies itself as a proxy to a website but hides its own identity. It does this by changing its IP address to an incorrect one.

Distorting proxies are a good choice for people who want to hide their location while accessing the internet. This type of proxy can make it look like you are browsing from a specific country and give you the advantage of hiding not just your identity but that of the proxy, too. This means even if you are associated with the proxy, your identity is still secure. However, some websites automatically block distorting proxies, which could keep an end-user from accessing sites they need.

Data Center Proxy

Data center proxies are not affiliated with an internet service provider (ISP) but are provided by another corporation through a data center. The proxy server exists in a physical data center, and the user's requests are routed through that server.

Data center proxies are a good choice for people who need quick response times and an inexpensive solution. They are therefore a good choice for people who need to gather intelligence on a person or organization very quickly. They carry the benefit of giving users the power to swiftly and inexpensively harvest data. On the other hand, they do not offer the highest level of anonymity, which may put users' information or identity at risk.

Residential Proxy

A residential proxy gives you an IP address that belongs to a specific, physical device. All requests are then channeled through that device.

Residential proxies are well-suited for users who need to verify the ads that go on their website, so you can block cookies, suspicious or unwanted ads from competitors or bad actors. Residential proxies are more trustworthy than other proxy options. However, they often cost more money to use, so users should carefully analyze whether the benefits are worth the extra investment.

Public Proxy

A public proxy is accessible by anyone free of charge. It works by giving users access to its IP address, hiding their identity as they visit sites.

Public proxies are best suited for users for whom cost is a major concern and security and speed are not. Although they are free and easily accessible, they are often slow because they get bogged down with free users. When you use a public proxy, you also run an increased risk of having your information accessed by others on the internet.

Shared Proxy

Shared proxies are used by more than one user at once. They give you access to an IP address that may be shared by other people, and then you can surf the internet while appearing to browse from a location of your choice.

Shared proxies are a solid option for people who do not have a lot of money to spend and do not necessarily need a fast connection. The main advantage of a shared proxy is its low cost. Because they are shared by others, you may get blamed for someone else's bad decisions, which could get you banned from a site.

SSL Proxy

A secure sockets layer (SSL) proxy provides decryption between the client and the server. As the data is encrypted in both directions, the proxy hides its existence from both the client and the server.

These proxies are best suited for organizations that need enhanced protection against threats that the SSL protocol reveals and stops. Because Google prefers servers that use SSL, an SSL proxy, when used in connection with a website, may help its search engine ranking. On the downside, content encrypted on an SSL proxy cannot be cached, so when visiting websites multiple times, you may experience slower performance than you would otherwise.

Rotating Proxy

A rotating proxy assigns a different IP address to each user that connects to it. As users connect, they are given an address that is unique from the device that connected before it.

Rotating proxies are ideal for users who need to do a lot of high-volume, continuous web scraping. They allow you to return to the same website again and again anonymously. However, you have to be careful when choosing rotating proxy services. Some of them contain public or shared proxies that could expose your data.

Reverse Proxy

Unlike a forward proxy, which sits in front of clients, a reverse proxy is positioned in front of web servers and forwards requests from a browser to the web servers. It works by intercepting requests from the user at the network edge of the web server. It then sends the requests to and receives replies from the origin server.

Reverse proxies are a strong option for popular websites that need to balance the load of many incoming requests. They can help an organization reduce bandwidth load because they act like another web server managing incoming requests. The downside is reverse proxies can potentially expose the HTTP server architecture if an attacker is able to penetrate it. This means network administrators may have to beef up or reposition their firewall if they are using a reverse proxy.

Proxy Server vs. VPN

On the surface, proxy servers and virtual private networks (VPNs) may seem interchangeable because they both route requests and responses through an external server. Both also allow you to access websites that would otherwise block the country you’re physically located in. However, VPNs provide better protection against hackers because they encrypt all traffic.

Choosing VPN or Proxy

If you need to constantly access the internet to send and receive data that should be encrypted or if your company has to reveal data you must hide from hackers and corporate spies, a VPN would be a better choice.

If an organization merely needs to allow its users to browse the internet anonymously, a proxy server may do the trick. This is the better solution if you simply want to know which websites team members are using or you want to make sure they have access to sites that block users from your country.

A VPN is better suited for business use because users usually need secure data transmission in both directions. Company information and personnel data can be very valuable in the wrong hands, and a VPN provides the encryption you need to keep it protected. For personal use where a breach would only affect you, a single user, a proxy server may be an adequate choice. You can also use both technologies simultaneously, particularly if you want to limit the websites that users within your network visit while also encrypting their communications.

Squid Proxy ?

squid proxy server is an open source Unix proxy server that stores Internet content in a cache that is geographically closer to the user making the request than the content's originating server. Squid can cache HTTP and FTP files, among many other types of Web content. Websites, media files, and other frequently requested content can benefit from caching to improve response times and alleviate network congestion.

Details about Squid Proxy Server

In most cases, a Squid proxy server will be set up on a machine that is not the primary Web server housing the original content. Squid is able to do its job by monitoring how frequently an object is accessed over a network. At first, Squid will play the role of an intermediate, forwarding requests from clients to servers while also caching a local copy of the resource being sought.

With Squid, the download is accelerated and bandwidth is conserved if the same client or numerous clients request the same information before it expired from Squid's cache.

When it comes to delivering rich media and streaming video, ISPs have been using Squid proxy servers since the early 1990s since they increase download speeds and decrease latency. Squid proxy servers are commonly used by website owners as a content accelerator, caching frequently visited information and reducing Web server demands.

Squid proxy servers are used by content providers and media businesses for load balancing and managing traffic spikes for popular material, ultimately benefiting the user experience of viewers seeking programming.

Squid is available for use without cost or restriction thanks to the Free Software Foundation's (FSF) General Public License (GPL). The squid was initially developed for Unix-based systems but has since been ported to Windows.

Squid was developed from the open-source Harvest Project, which was supported by the Advanced Research Projects Agency (ARPA). When work in the different direction first started, we gave the project the code name "Squid" to set it apart.

Advantages of a Squid Proxy Cache Server

Among the many benefits of using a Squid Proxy Server are:

* Web caching is the practise of storing data on a local server rather than sending each request to the Internet, which greatly increases the speed at which a web server can process requests.
* Squid Proxy Cache Server can function as a Domain Name System (DNS) server, resolving hostnames with its own internal DNS client or with the assistance of external DNS applications.
* Squid is a useful security tool because it may block unwelcome visitors from entering a network and prevent dangerous websites from harming users who accidentally click on hazardous links.
* Squid Proxy can be set up to share loads across hierarchies of proxy servers, allowing for better response times and decongestion of traffic in the event of a traffic spike or unexpected bandwidth clogging (perhaps while backups are being done).

* Security Squid's authentication options include defining an Access Control List (ACL) that determines which users are authorized to use the proxy's resources.
* Squid can also function as a proxy server, granting or denying users access to the internet depending on a variety of factors, including the time of day.
* Statistics about commonly visited websites, for instance, can be utilised to evaluate users' browsing behavior through the reports generated by Squid Proxy, which can be used as input for scaling, security, and resource planning.

Assignments:11

Module:- COSA(Proxy Server and squid proxy)

Name:- Prithviraj Nikam

Lab Assignment :-

In my case

Proxy Server :-192.168.3.47

Client as Centos:-192.168.3.137

Client as Windows 10:-192.168.3.131

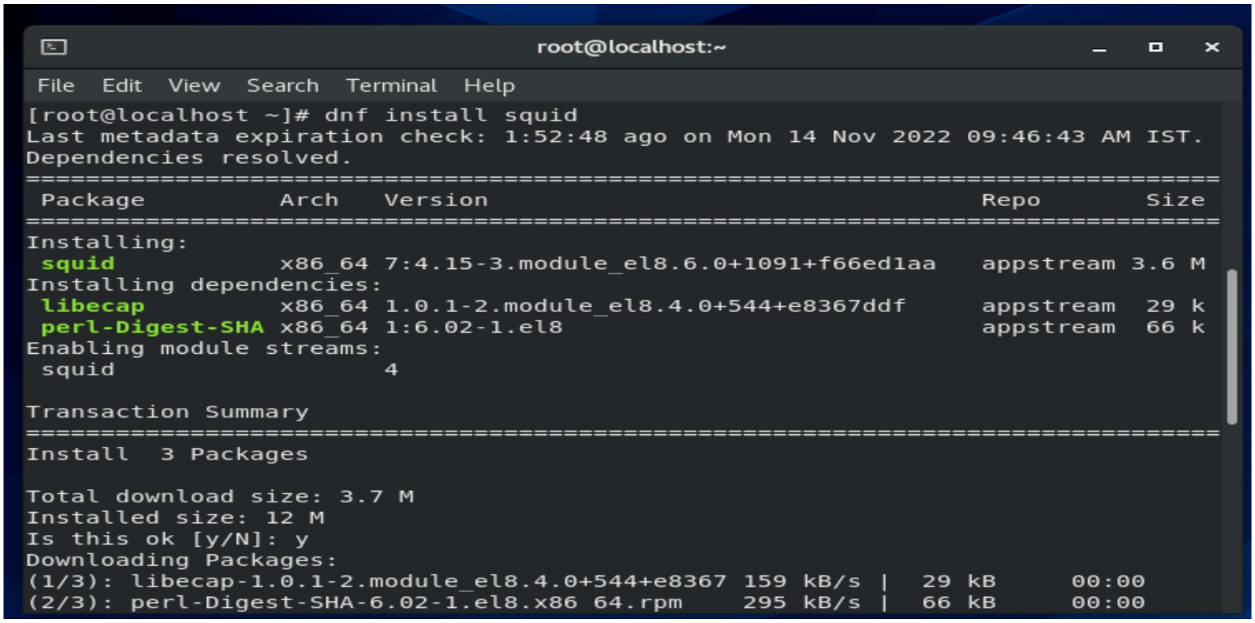
Installation and configuration of Squid Proxy server

Step-1:- Step 1:- Install the squid packages

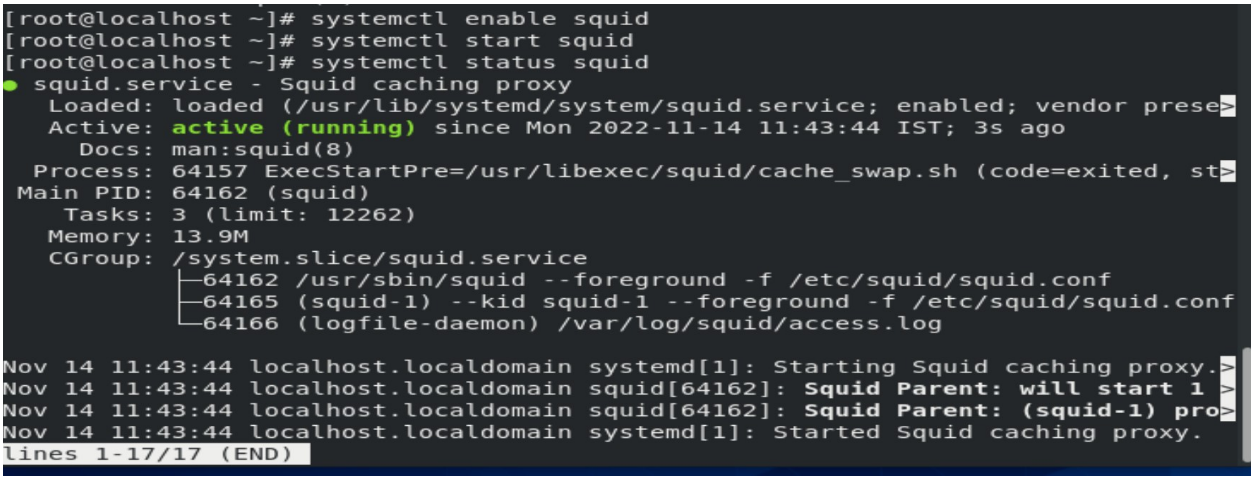
# dnf install –y squid*

# systemctl enable squid.service –now

#systemctl status squid.service



```
[root@localhost ~]# dnf install squid
Last metadata expiration check: 1:52:48 ago on Mon 14 Nov 2022 09:46:43 AM IST.
Dependencies resolved.
================================================================================
 Package          Arch   Version                                 Repo      Size
================================================================================
Installing:
 squid            x86_64 7:4.15-3.module_el8.6.0+1091+f66ed1aa   appstream 3.6 M
Installing dependencies:
 libecap          x86_64 1.0.1-2.module_el8.4.0+544+e8367ddf     appstream  29 k
 perl-Digest-SHA  x86_64 1:6.02-1.el8                            appstream  66 k
Enabling module streams:
 squid                   4

Transaction Summary
================================================================================
Install  3 Packages

Total download size: 3.7 M
Installed size: 12 M
Is this ok [y/N]: y
Downloading Packages:
(1/3): libecap-1.0.1-2.module_el8.4.0+544+e8367 159 kB/s |  29 kB     00:00
(2/3): perl-Digest-SHA-6.02-1.el8.x86_64.rpm    295 kB/s |  66 kB     00:00
```



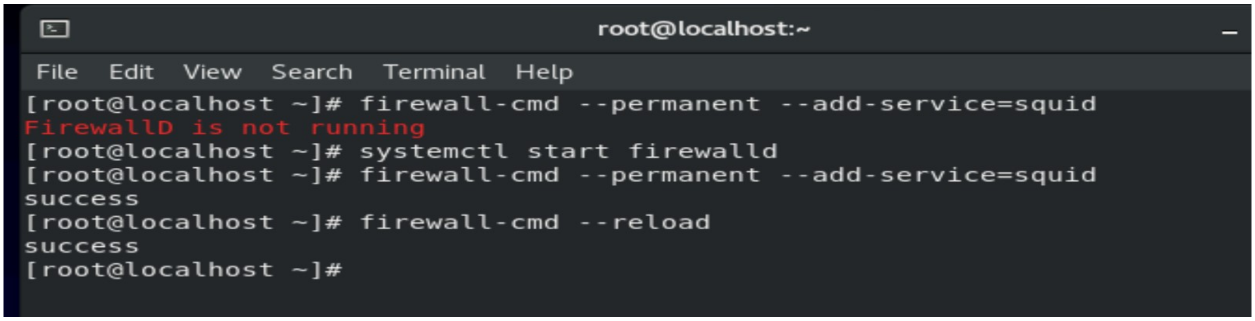
```
[root@localhost ~]# systemctl enable squid
[root@localhost ~]# systemctl start squid
[root@localhost ~]# systemctl status squid
● squid.service - Squid caching proxy
   Loaded: loaded (/usr/lib/systemd/system/squid.service; enabled; vendor prese>
   Active: active (running) since Mon 2022-11-14 11:43:44 IST; 3s ago
     Docs: man:squid(8)
  Process: 64157 ExecStartPre=/usr/libexec/squid/cache_swap.sh (code=exited, st>
 Main PID: 64162 (squid)
    Tasks: 3 (limit: 12262)
   Memory: 13.9M
   CGroup: /system.slice/squid.service
           ├─64162 /usr/sbin/squid --foreground -f /etc/squid/squid.conf
           ├─64165 (squid-1) --kid squid-1 --foreground -f /etc/squid/squid.conf
           └─64166 (logfile-daemon) /var/log/squid/access.log

Nov 14 11:43:44 localhost.localdomain systemd[1]: Starting Squid caching proxy.>
Nov 14 11:43:44 localhost.localdomain squid[64162]: Squid Parent: will start 1 >
Nov 14 11:43:44 localhost.localdomain squid[64162]: Squid Parent: (squid-1) pro>
Nov 14 11:43:44 localhost.localdomain systemd[1]: Started Squid caching proxy.
lines 1-17/17 (END)
```

Step-2:- If firewall enable:-

Add the rule in the firewall for squid

# firewall-cmd --permanent --add-service=squid

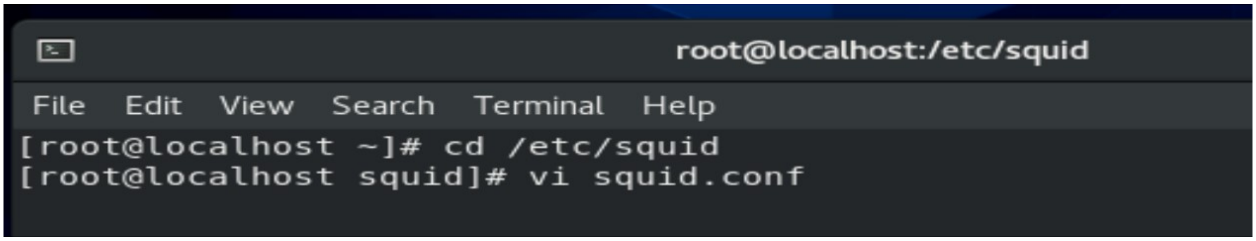
# firewall-cmd -- reload



```
[root@localhost ~]# firewall-cmd --permanent --add-service=squid
FirewallD is not running
[root@localhost ~]# systemctl start firewalld
[root@localhost ~]# firewall-cmd --permanent --add-service=squid
success
[root@localhost ~]# firewall-cmd --reload
success
[root@localhost ~]#
```

Step-3:- Add the rules in configuration file of squid.conf

vim /etc/squid/squid.conf


root@localhost:/etc/squid
File Edit View Search Terminal Help

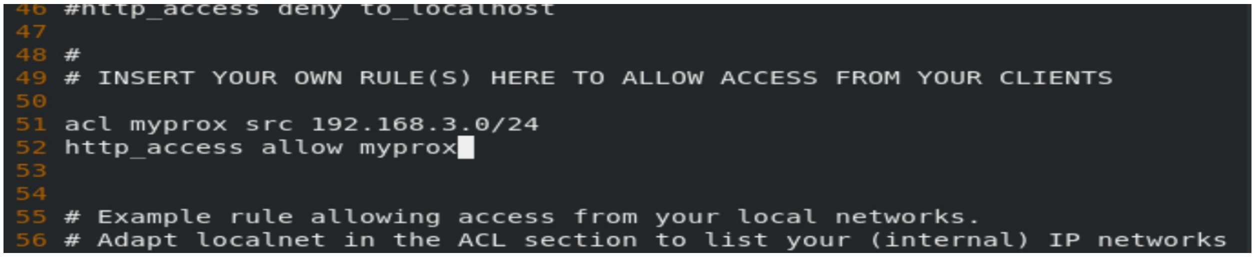
```
[root@localhost ~]# cd /etc/squid
[root@localhost squid]# vi squid.conf
```

Step-4:- Below the line number 49

Now we want to allow internet connection for our network.

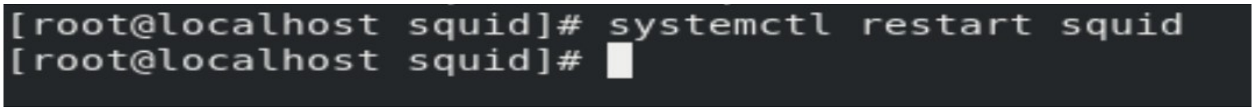
acl mynetwork src 192.168.3.0/24

http_access allow mynetwork



```
46 #http_access deny to_localhost
47
48 #
49 # INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
50
51 acl myprox src 192.168.3.0/24
52 http_access allow myprox
53
54
55 # Example rule allowing access from your local networks.
56 # Adapt localnet in the ACL section to list your (internal) IP networks
```

Restart the service:-

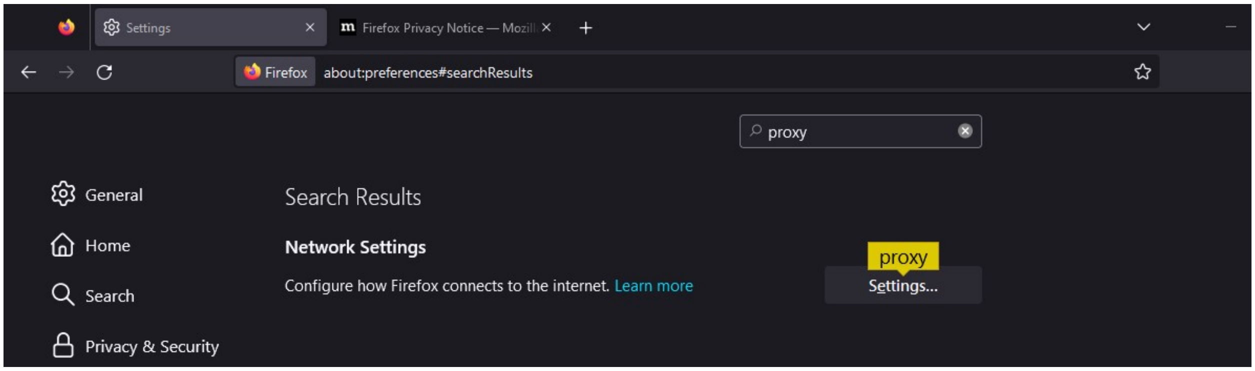


```
[root@localhost squid]# systemctl restart squid
[root@localhost squid]# 
```

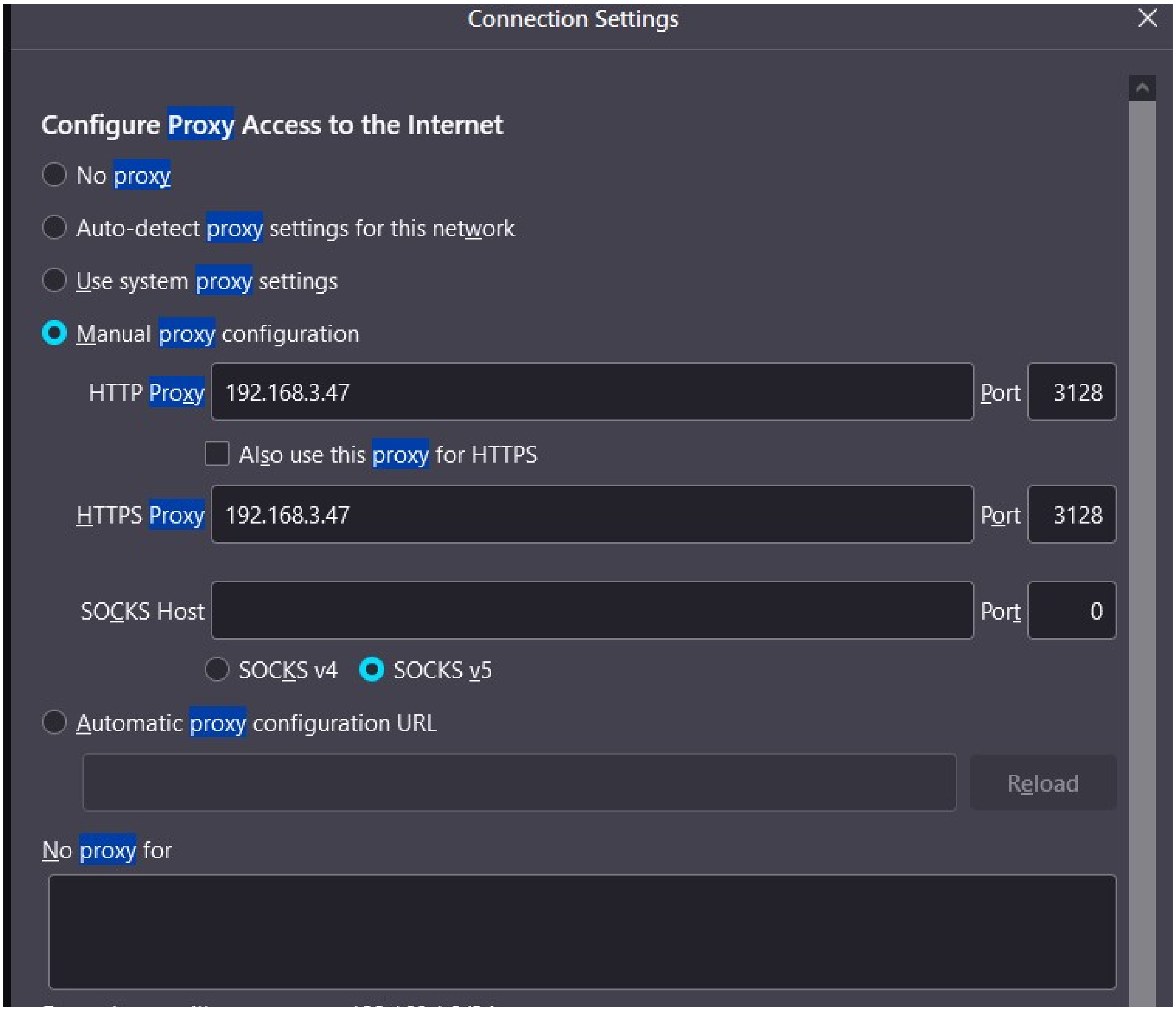
Step-5:- After restart the squid configure your client machine.

On Windows:

Open mozilla browser Go to Setting search proxy Enter the proxy server detail



Configure how Firefox connects to the internet. Learn more



Connection Settings

Configure Proxy Access to the Internet

○ No proxy

○ Auto-detect proxy settings for this network

○ Use system proxy settings

● Manual proxy configuration

HTTP Proxy 192.168.3.47 Port 3128

□ Also use this proxy for HTTPS

HTTPS Proxy 192.168.3.47 Port 3128

SOCKS Host Port 0

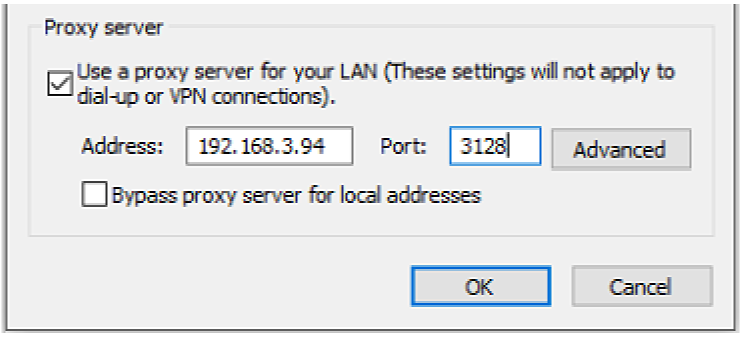
○ SOCKS v4 ● SOCKS v5

○ Automatic proxy configuration URL

No proxy for

Or

Open Internet OptionsGo to Connection tabClick on LAN settingsin proxy server fill the details as like below the image and press “OK”



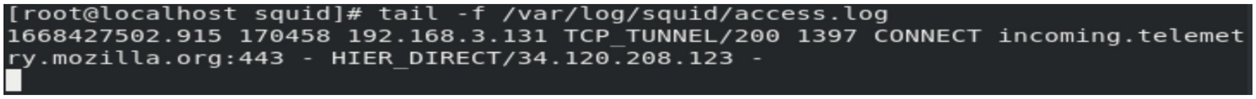
Proxy server

☑ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: 192.168.3.94 Port: 3128

□ Bypass proxy server for local addresses

Step-6:-Log detail of the Squid server



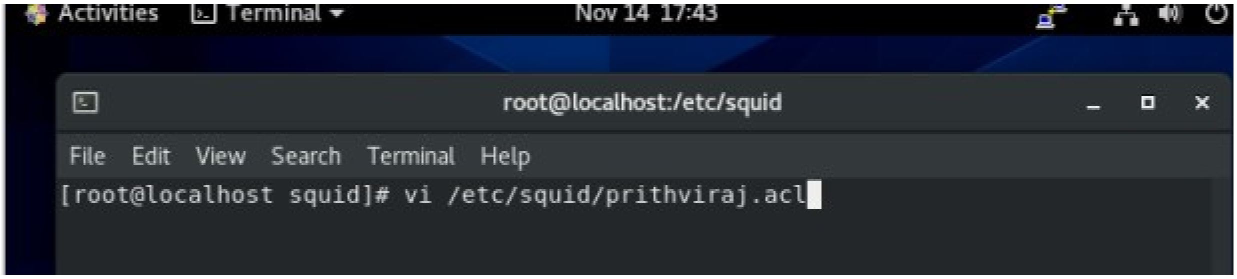
```
[root@localhost squid]# tail -f /var/log/squid/access.log
1668427502.915 170458 192.168.3.131 TCP_TUNNEL/200 1397 CONNECT incoming.telemet
ry.mozilla.org:443 - HIER_DIRECT/34.120.208.123 -
```

Step-7 :- Try to block certain web sites through the squid proxy:-

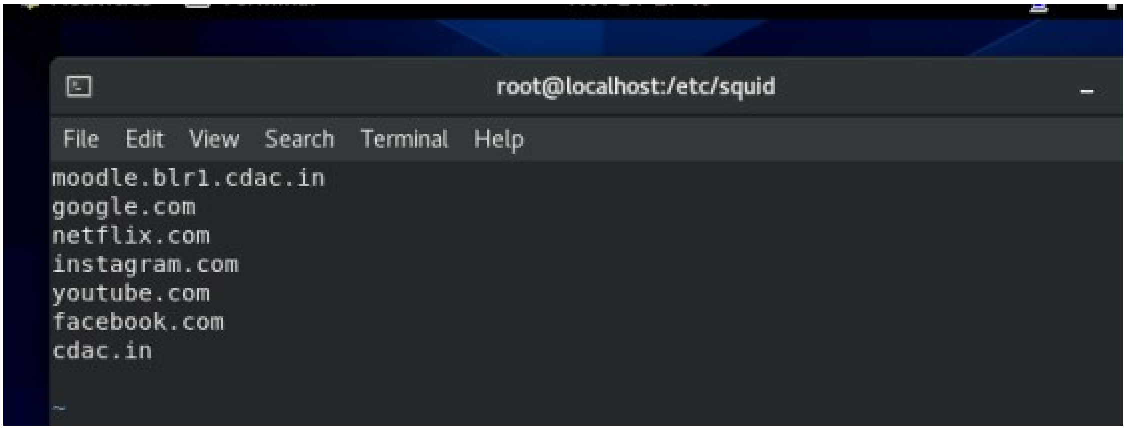
Create a file with “prithviraj.acl”

Location of file /etc/squid/ prithviraj.acl

Vi /etc/squid/prithviraj.acl

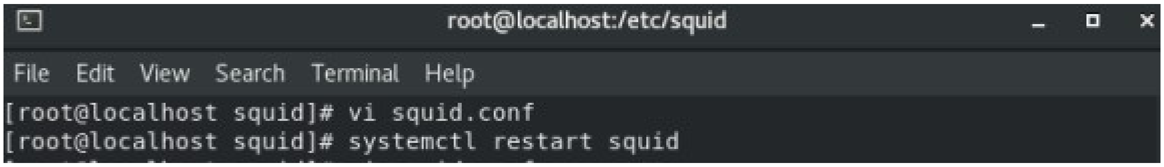


```
[root@localhost squid]# vi /etc/squid/prithviraj.acl
```

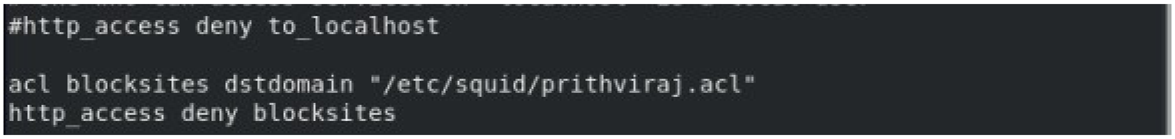

root@localhost:/etc/squid
File Edit View Search Terminal Help

```
moodle.blr1.cdac.in
google.com
netflix.com
instagram.com
youtube.com
facebook.com
cdac.in

~
```

Step-8:- Add the rule as below in squid.conf file
vi /etc/squid/squid.conf
Then restart it

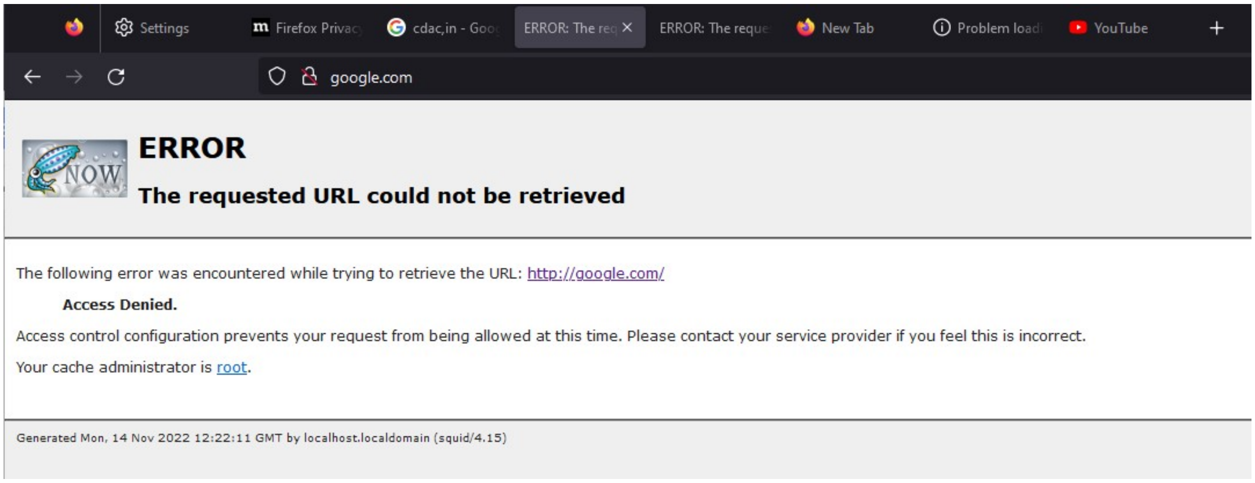

root@localhost:/etc/squid
File Edit View Search Terminal Help

```
[root@localhost squid]# vi squid.conf
[root@localhost squid]# systemctl restart squid
```



```
#http_access deny to_localhost

acl blocksites dstdomain "/etc/squid/prithviraj.acl"
http_access deny blocksites
```

Step-9:- To check on browser and type the websites
google.com



ERROR

The requested URL could not be retrieved

The following error was encountered while trying to retrieve the URL: http://google.com/

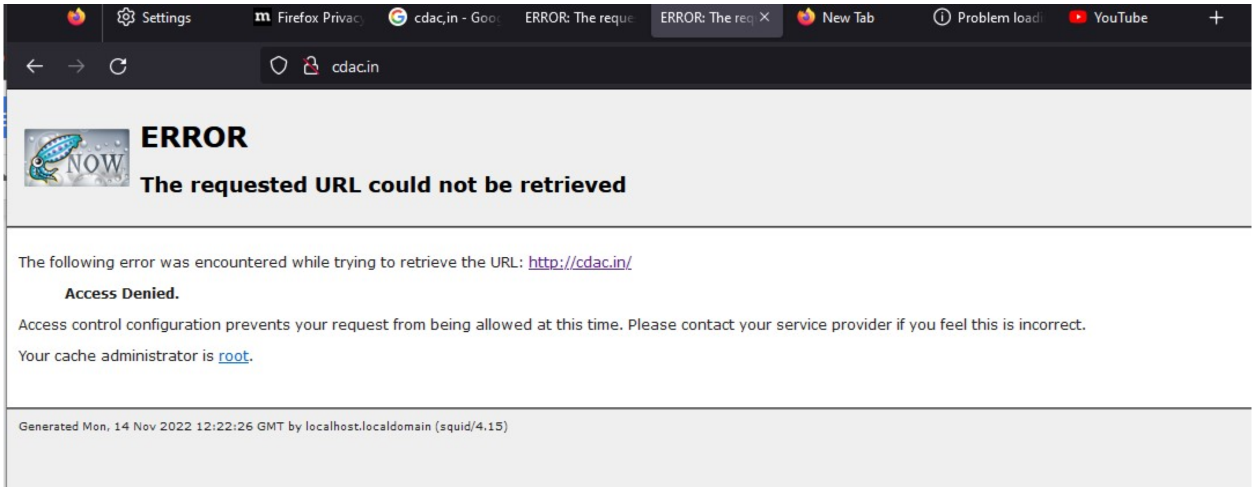
Access Denied.

Access control configuration prevents your request from being allowed at this time. Please contact your service provider if you feel this is incorrect.

Your cache administrator is root.

Generated Mon, 14 Nov 2022 12:22:11 GMT by localhost.localdomain (squid/4.15)

Cdac.in



ERROR

The requested URL could not be retrieved

The following error was encountered while trying to retrieve the URL: http://cdac.in/

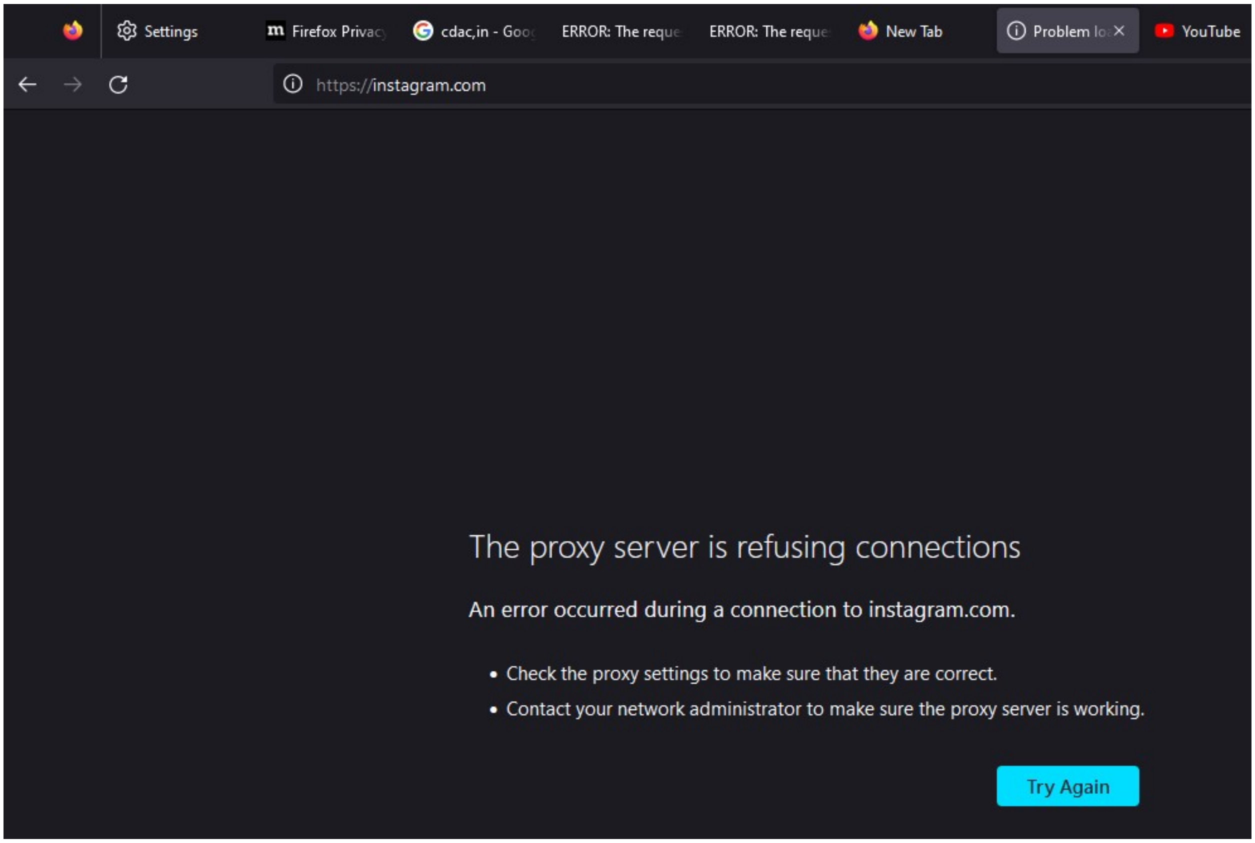
Access Denied.

Access control configuration prevents your request from being allowed at this time. Please contact your service provider if you feel this is incorrect.

Your cache administrator is root.

Generated Mon, 14 Nov 2022 12:22:26 GMT by localhost.localdomain (squid/4.15)

instagram.com

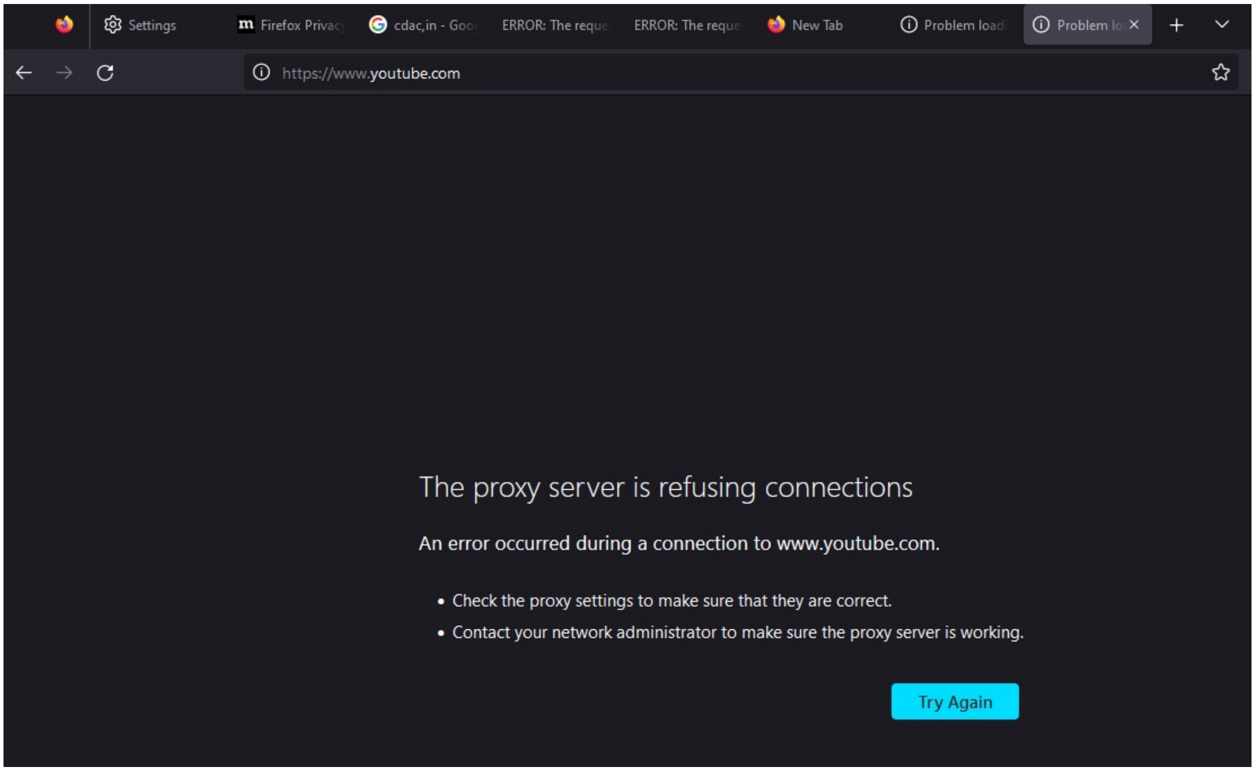


The proxy server is refusing connections

An error occurred during a connection to instagram.com.

- Check the proxy settings to make sure that they are correct.
- Contact your network administrator to make sure the proxy server is working.

Youtube.com

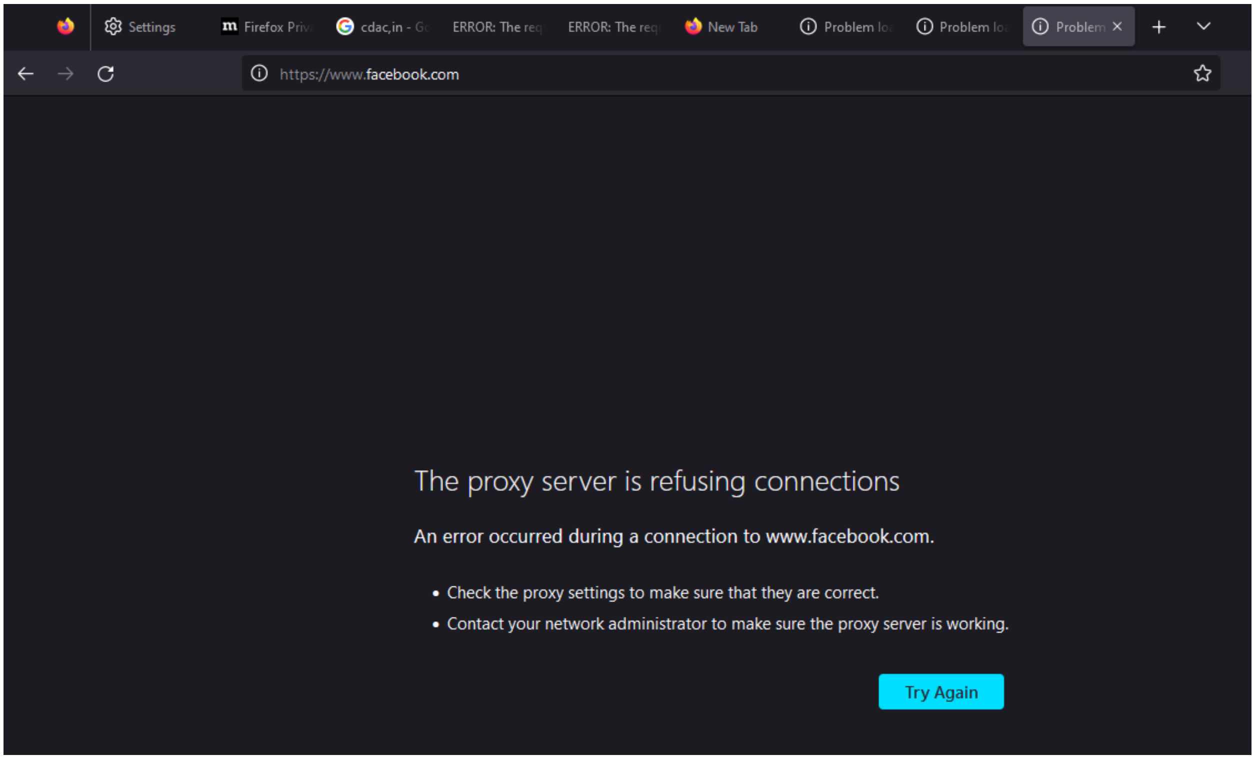


The proxy server is refusing connections

An error occurred during a connection to www.youtube.com.

- Check the proxy settings to make sure that they are correct.
- Contact your network administrator to make sure the proxy server is working.

Facebook

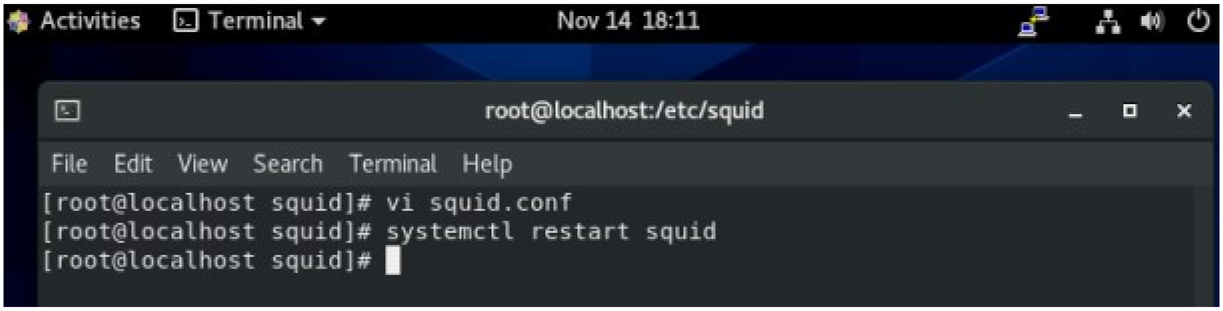


The proxy server is refusing connections

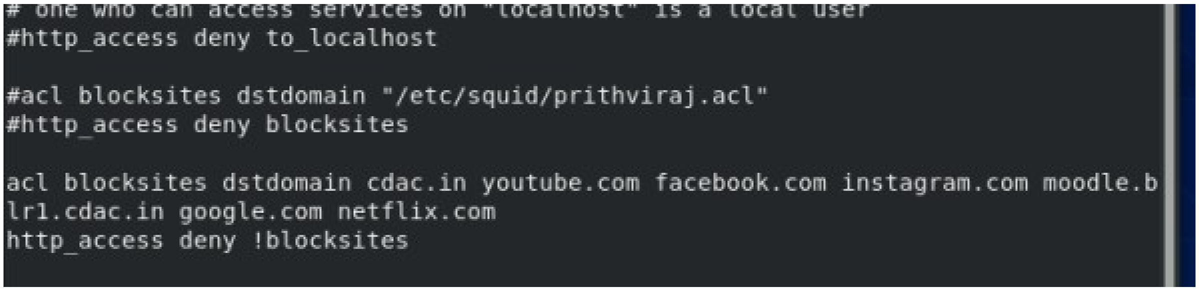
An error occurred during a connection to www.facebook.com.

- Check the proxy settings to make sure that they are correct.
- Contact your network administrator to make sure the proxy server is working.

Step-10:- (2)Other method

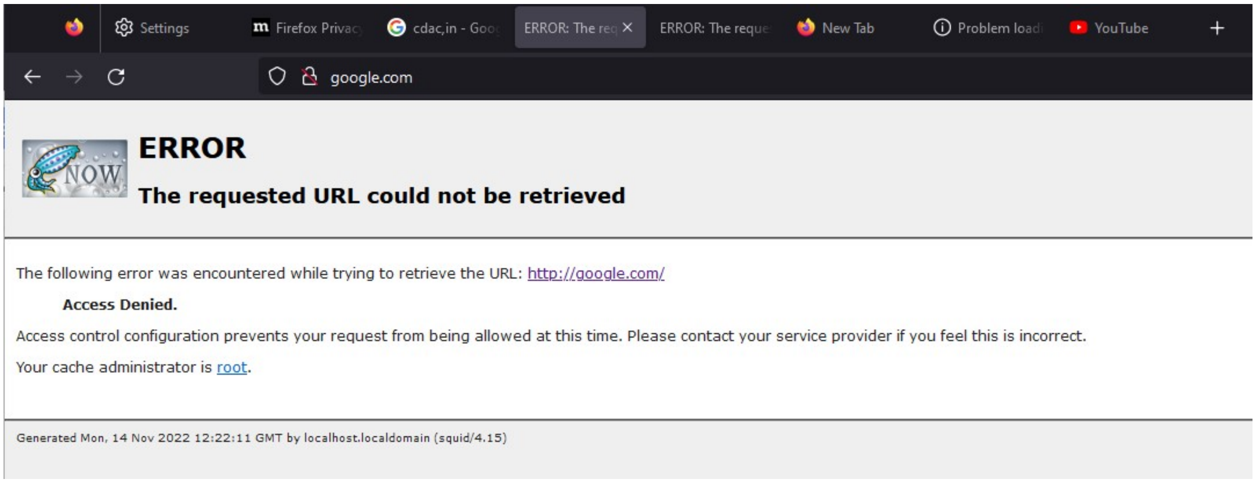

Activities
Terminal
Nov 14 18:11
root@localhost:/etc/squid
File Edit View Search Terminal Help

```
[root@localhost squid]# vi squid.conf
[root@localhost squid]# systemctl restart squid
[root@localhost squid]# 
```



```
# one who can access services on "localhost" is a local user
#http_access deny to_localhost

#acl blocksites dstdomain "/etc/squid/prithviraj.acl"
#http_access deny blocksites

acl blocksites dstdomain cdac.in youtube.com facebook.com instagram.com moodle.b
lr1.cdac.in google.com netflix.com
http_access deny !blocksites
```

Step-11:- To check on browser and type the websites google.com



ERROR

The requested URL could not be retrieved

The following error was encountered while trying to retrieve the URL: http://google.com/

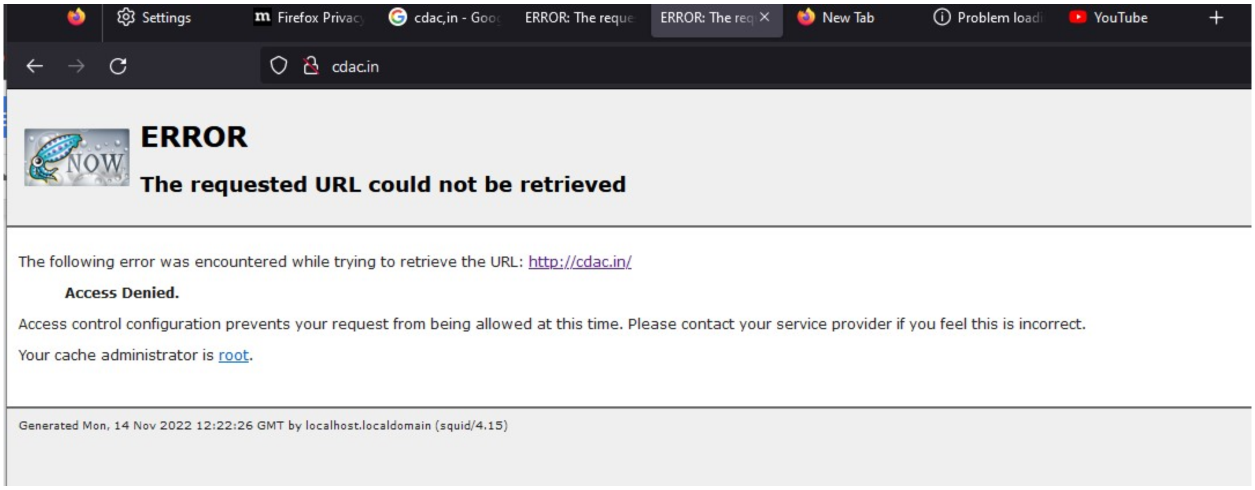
Access Denied.

Access control configuration prevents your request from being allowed at this time. Please contact your service provider if you feel this is incorrect.

Your cache administrator is root.

Generated Mon, 14 Nov 2022 12:22:11 GMT by localhost.localdomain (squid/4.15)

Cdac.in



ERROR

The requested URL could not be retrieved

The following error was encountered while trying to retrieve the URL: http://cdac.in/

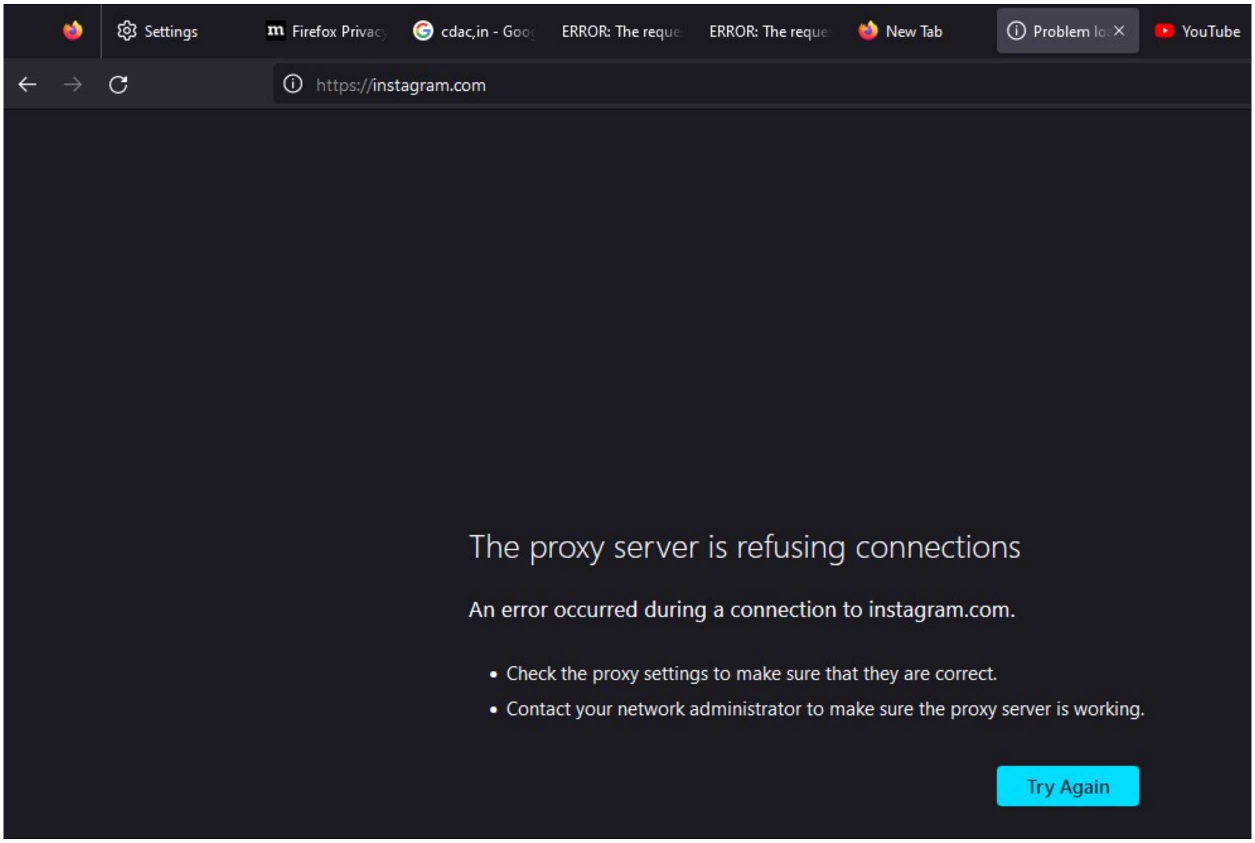
Access Denied.

Access control configuration prevents your request from being allowed at this time. Please contact your service provider if you feel this is incorrect.

Your cache administrator is root.

Generated Mon, 14 Nov 2022 12:22:26 GMT by localhost.localdomain (squid/4.15)

instagram.com

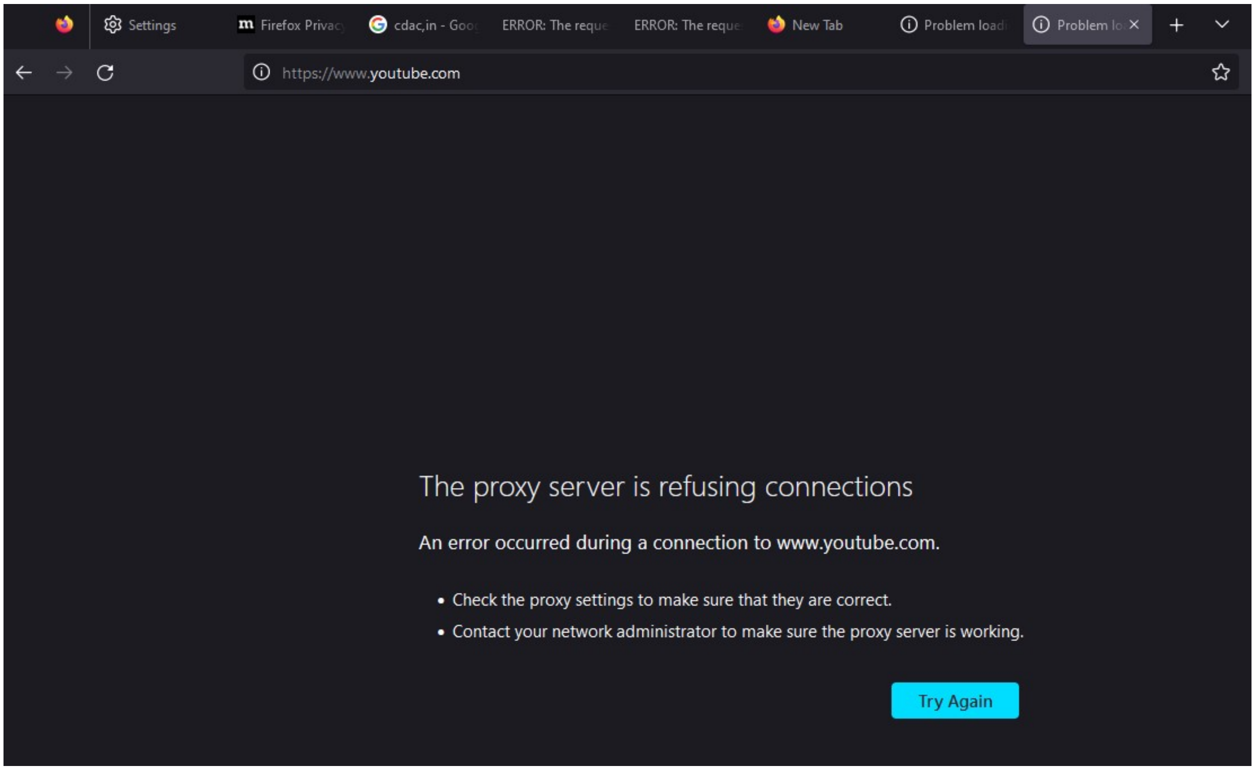


The proxy server is refusing connections

An error occurred during a connection to instagram.com.

- Check the proxy settings to make sure that they are correct.
- Contact your network administrator to make sure the proxy server is working.

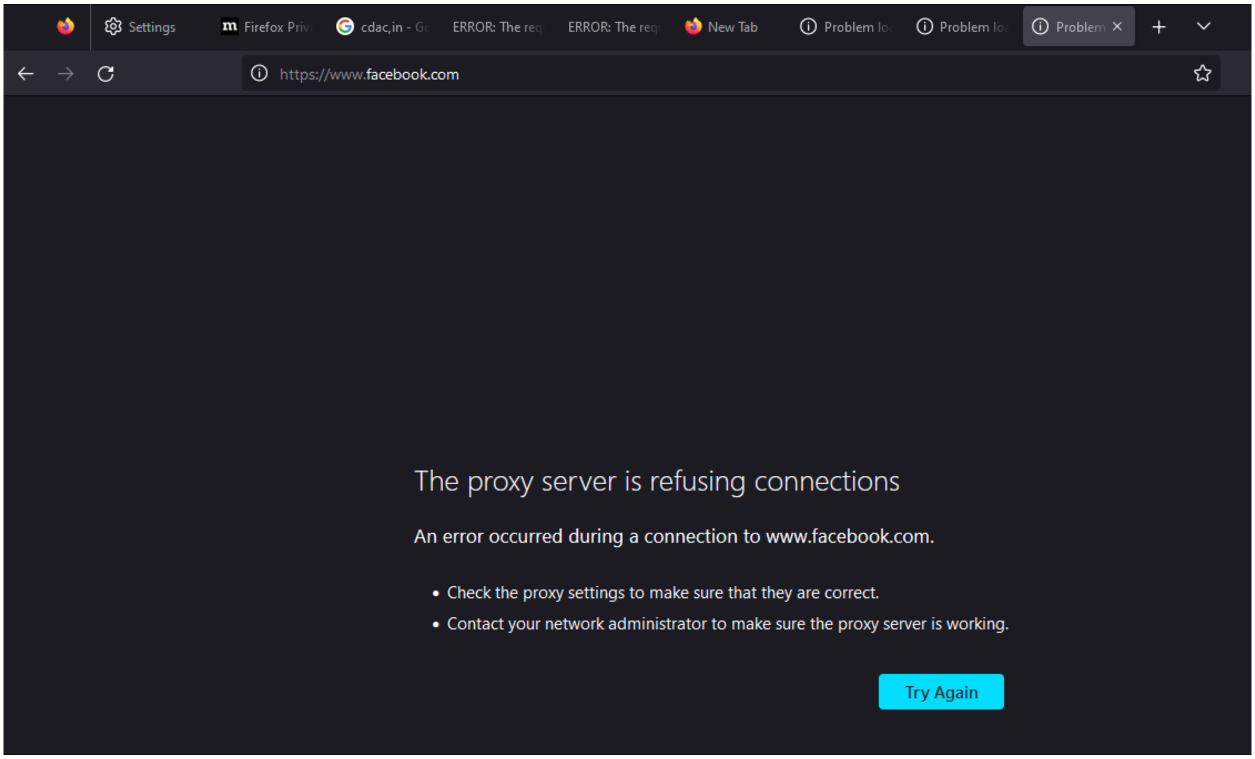
Youtube.com



The proxy server is refusing connections

An error occurred during a connection to www.youtube.com.

- Check the proxy settings to make sure that they are correct.
- Contact your network administrator to make sure the proxy server is working.



The proxy server is refusing connections

An error occurred during a connection to www.facebook.com.

- Check the proxy settings to make sure that they are correct.
- Contact your network administrator to make sure the proxy server is working.