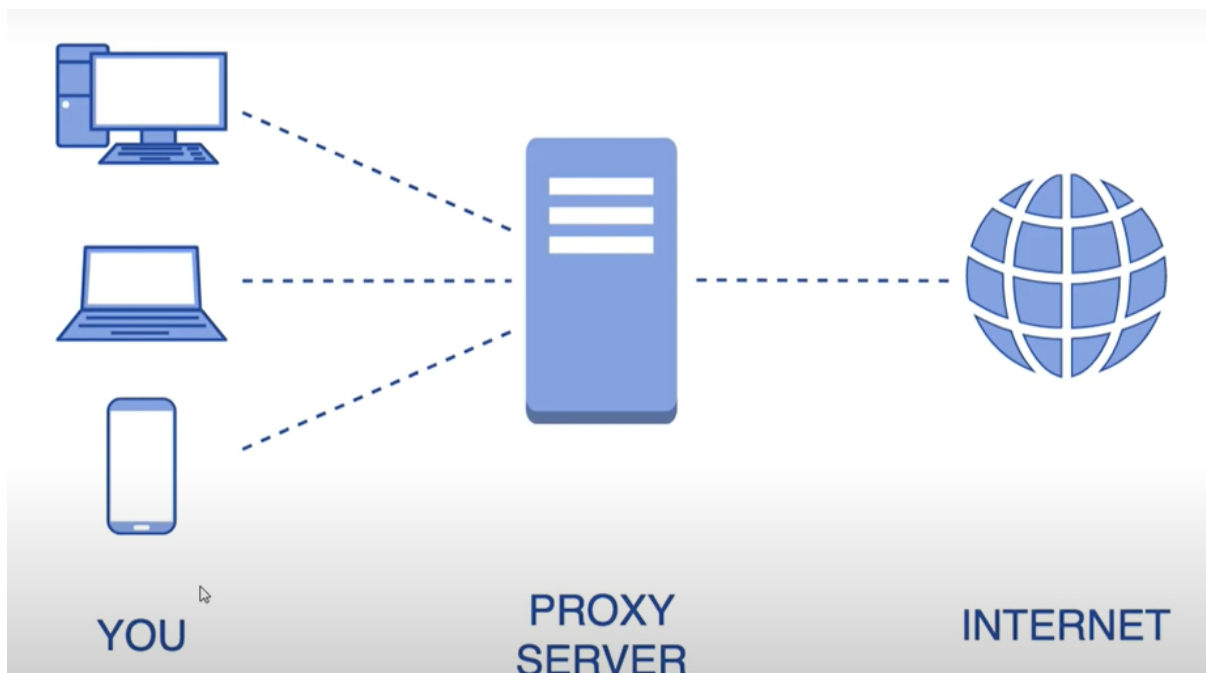


How to Install & Configure Squid Proxy Server

Definition: - SQUID proxy server is used to filter web traffic and reducing the unwanted/unauthorized website access and we can also limit the bandwidth.

Diagram: -



Installation Steps: -

Step 1: - Install squid

- **yum install squid**

Step 2: - Start and enable squid server.

- **systemctl enable squid && systemctl start squid**
OR
- **systemctl enable-now squid**

Step 3: - Check the status of squid server.

➤ **systemctl status squid**

```
[root@ip-13-0-1-4 ~]# systemctl status squid
● squid.service - Squid caching proxy
   Loaded: loaded (/usr/lib/systemd/system/squid.service; disabled; vendor preset: disabled)
   Active: active (running) since Mon 2022-02-21 12:16:01 UTC; 2min 50s ago
     Process: 20714 ExecStop=/usr/sbin/squid -k shutdown -f $SQUID_CONF (code=exited, status=0/SUCCESS)
     Process: 20723 ExecStart=/usr/sbin/squid $SQUID_OPTS -f $SQUID_CONF (code=exited, status=0/SUCCESS)
     Process: 20718 ExecStartPre=/usr/libexec/squid/cache_swap.sh (code=exited, status=0/SUCCESS)
    Main PID: 20726 (squid)
      CGroup: /system.slice/squid.service
              └─20726 /usr/sbin/squid -f /etc/squid/squid.conf
                  └─20728 (squid-1) -f /etc/squid/squid.conf
                      └─20729 (logfile-daemon) /var/log/squid/access.log

Feb 21 12:16:01 ip-13-0-1-4.ap-south-1.compute.internal systemd[1]: Starting Squid caching proxy...
Feb 21 12:16:01 ip-13-0-1-4.ap-south-1.compute.internal squid[20726]: Squid Parent: will start 1 kids
Feb 21 12:16:01 ip-13-0-1-4.ap-south-1.compute.internal squid[20726]: Squid Parent: (squid-1) process 20728 started
Feb 21 12:16:01 ip-13-0-1-4.ap-south-1.compute.internal systemd[1]: Started Squid caching proxy.
[root@ip-13-0-1-4 ~]#
```

Blocking Websites: -

➤ **Blocking a specific URL**

Step 1: - Create a file named with **blocked_sites**.

Step 2: - Add the websites to be blocked in the file. For example,

➤ **vi /etc/squid/blocked_sites**

.facebook.com

.twitter.com

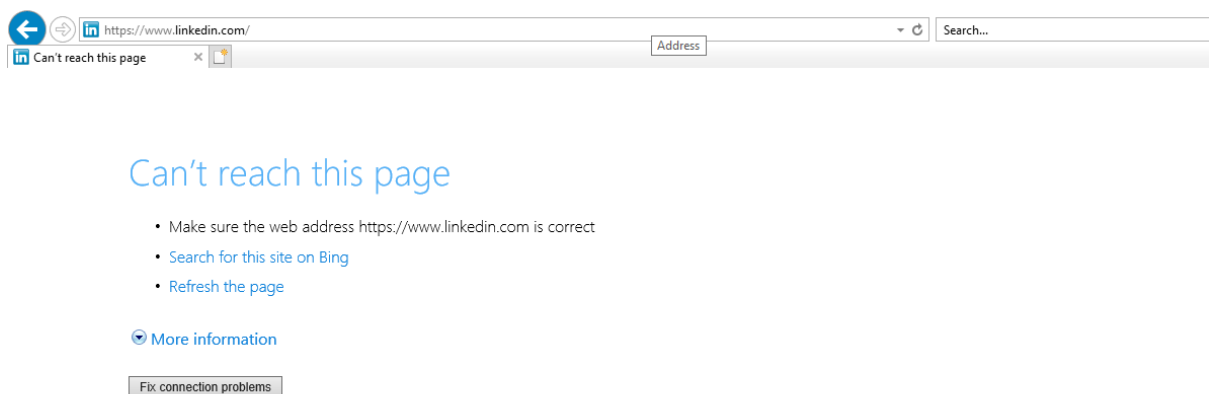
.instagram.com

.youtube.com

.linkedin.com

```
[root@ip-13-0-1-4 ~]# cat /etc/squid/blocked_sites
.youtube.com
.facebook.com
.linkedin.com
.instagram.com
.twitter.com
[root@ip-13-0-1-4 ~]#
```

Output: -



Allowing Websites: -

➤ **ALLOW only specific URL**

Step 1: - Open a file named with **allowed_sites**.

Step 2: - Add the websites to be allowed in the file. For example,

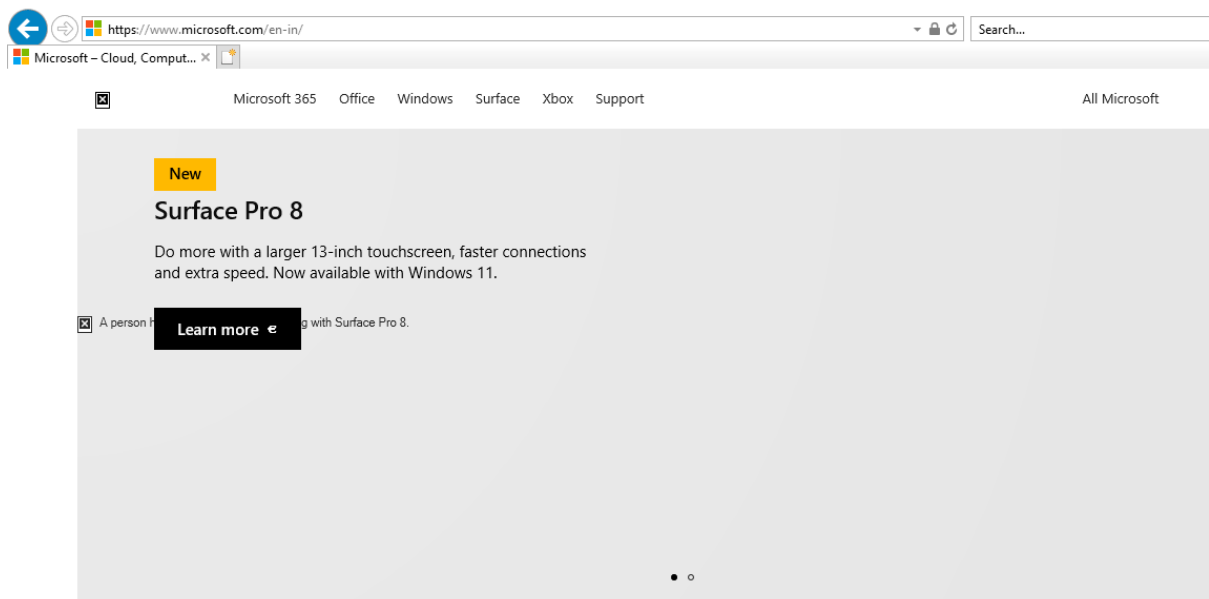
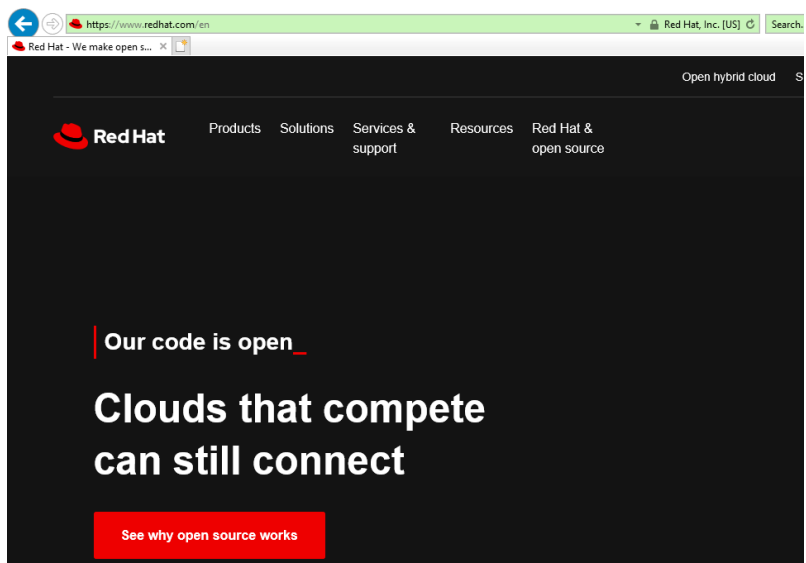
➤ **vi /etc/squid/allowed_sites**

.microsoft.com

.redhat.com

```
[root@ip-13-0-1-4 squid]#  
[root@ip-13-0-1-4 squid]# cat allowed_sites  
.microsoft.com  
.redhat.com  
[root@ip-13-0-1-4 squid]#  
[root@ip-13-0-1-4 squid]#  
[root@ip-13-0-1-4 squid]#
```

Output: -



Block only http requests: -

➤ Block HTTP requests.

Step 1: - Open the file named squid.conf and add the below path

```
acl allow_url dstdomain "/etc/squid/allowed_sites"  
http_access allow allow_url
```

Step 2 : - To block only http requests.

```
change the http_access allow to deny  
http_access allow all > http_access deny all
```

```
acl allow_url dstdomain "/etc/squid/allowed_sites"  
http_access allow allow_url  
  
# Example rule allowing access from your local networks.  
# Adapt localnet in the ACL section to list your (internal) IP networks  
# from where browsing should be allowed  
#http_access allow localnet  
#http_access allow localhost  
  
# And finally deny all other access to this proxy  
http_access deny all  
  
# Squid normally listens to port 3128  
http_port 3128
```

Output: -

