

# SETTING UP PROXY CHACHING SERVER IN CENTOS

---

## squid proxy caching server install (server side configuration steps)

---

1) update the repository in centos

=> **yum update -y**

2) install squid packages

=> **yum install squid -y**

3) enable and start the squid service in boot time

=> **systemctl enable squid**

=> **systemctl start squid**

4) check the status of the process

=> **systemctl status squid**

5) Edit the squid configuration file in This configuration

→ we can write acl for the client who can use the proxy server

→ we can select the cache memory

→ allow or deny specific network for using acl

→ block or allow specific website for the proxy server client

=> **vim /etc/squid/squid.conf**

\* by default squid listen to the port 3128 you can change it and set a different port. If we want to change the port we have to change the line `http_port` and specify the new port

```
# Squid normally listens to port 3128
http_port 3128

# Uncomment and adjust the following to add a disk cache directory
#cache_dir ufs /var/spool/squid 100 16 256

# Leave coredumps in the first cache dir
```

---

**`http_port` : port**

---

you can control the access of the squid server with acl (Access Control List)

you can create a text file with the list of the ip address with the allowed ip address and include with the acl and deny all other ip address that will prevent the other client to connect to the proxy server.

\* create a file with allowed ip address name **“`allowed_ips.txt`”**

**=>`vim allowed_ips.txt`**

---

**`192.168.x.x`**

**`192.168.x.x`**

192.168.x.x  
192.168.x.x  
192.168.x.x

---

\*now add the file to the acl .

```
#  
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS  
#  
acl Allowed_ips src "/etc/squid/allowed_ips.txt"  
http_access allow Allowed_ips
```

=> **vim /etc/squid/squid.conf**

---

**## syntax**

**#acl <name> src "<filepath>"**  
**#http\_access allow <name>**

**acl Allowed\_ips src '/etc/squid/allowed\_ips.txt'**  
**http\_access allow Allowed\_ips**

---

or you can give access to all the client by allowing all the clients

```
# 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
#http_access allow allowed_ips
# And finally deny all other access to this proxy
http_access allow all
```

---

## **http\_access allow all**

---

after changing the configuration we have to restart the service so that the configuration change successfully loaded.

**=>systemctl restart squid**

## **MONITOR USER ACCESS AND CACHE OF THE SERVER**

---

### **1) monitor the access of the user**

we go to the file **‘/var/log/squid/access.log’**

**=> tail -f access.log**

**=> cat -f access.log | more**

### **2) monitor the cache of the user**

we go to the file **‘/var/log/squid/cache.log’**

=> **tail -f cache.log**

=> **cat -f cache.log | more**

Thats the basic configuration of setting a squid proxy server in centos 7.