Most of command to that use after zabbix\_server restart

systemctl start squid.service

systemctl start snmpd.service

Configure Squid to Start on Boot and then start Squid:

systemctl start squid

Be sure that Squid starts at boot:

systemctl enable squid

To check the status of Squid:

systemctl status squid

To stop Squid:

systemctl stop squid

Start squid service and make it available on startup.

service squid start

chkconfig squid on

**Step 1:**

To install squid RPM and dependencies using the yum command.

yum install squid -y

**Sample Output:**

Installed:  
squid.x86\_64 7:3.3.8-11.el7Dependency Installed:  
libecap.x86\_64 0:0.2.0-8.el7  
perl-Compress-Raw-Bzip2.x86\_64 0:2.061-3.el7  
perl-Compress-Raw-Zlib.x86\_64 1:2.061-4.el7  
perl-DBI.x86\_64 0:1.627-4.el7  
perl-Data-Dumper.x86\_64 0:2.145-3.el7  
perl-Digest.noarch 0:1.17-245.el7  
perl-Digest-MD5.x86\_64 0:2.52-3.el7  
perl-IO-Compress.noarch 0:2.061-2.el7  
perl-Net-Daemon.noarch 0:0.48-5.el7  
perl-PlRPC.noarch 0:0.2020-14.el7

Squid is installed successfully from RPM, by default squid generate its configuration file under /etc/squid directory.

**Step 2:**

Let’s perform steps for basic configuration:

* Allow our network in acl.
* Add visible hostname

Edit squid.conf file which is located here /etc/squid/squid.conf  
Its recommended to create backup of default configuration file to be on safe side.

cp /etc/squid/squid.conf /etc/squid/squid.conf.org.back

Now open config file in vi text editor.

vi /etc/squid/squid.conf

Add 192.168.2.0/24 network as follows

acl broexperts\_network src 192.168.2.0/24  
http\_access allow broexperts\_network

change here below

vi /etc/squid/squid.conf

# Recommended minimum configuration:

#

# Example rule allowing access from your local networks.

# Adapt to list your (internal) IP networks from where browsing

# should be allowed

acl localnet src 10.0.0.0/8 # RFC1918 possible internal network

acl localnet src 172.16.0.0/12 # RFC1918 possible internal network

acl localnet src 192.168.5.0/24 # RFC1918 possible internal network

acl localnet src fc00::/7 # RFC 4193 local private network range

acl localnet src fe80::/10 # RFC 4291 link-local (directly plugged) machines

#main command that allow to open only specific websites.

acl GOOD dst allcad.intervalsonline.com be19.https.cdn.softlayer.net www.google-analytics.com w0.s.myintervals.com repo1.maven.org

repo.maven.apache.org mvnrepository.com 192.168.5.0/24

http\_access allow GOOD

http\_access deny all

Un-comment and adjust the following to add cache directory.

cache\_dir ufs /usr/local/squid/var/cache/squid 100 16 256

And at the last of config file add visible hostname

visible\_hostname pxy.broexperts.com

See below my recommended minimum squid.conf file:

# Recommended minimum configuration:  
# Adapt to list your (internal) IP networks from where browsing  
# should be allowedacl broexperts\_network src 192.168.2.0/24

acl SSL\_ports port 443  
acl Safe\_ports port 80 # http  
acl Safe\_ports port 21 # ftp  
acl Safe\_ports port 443 # https  
acl Safe\_ports port 70 # gopher  
acl Safe\_ports port 210 # wais  
acl Safe\_ports port 1025-65535 # unregistered ports  
acl Safe\_ports port 280 # http-mgmt  
acl Safe\_ports port 488 # gss-http  
acl Safe\_ports port 591 # filemaker  
acl Safe\_ports port 777 # multiling http  
acl CONNECT method CONNECT

#  
# Recommended minimum Access Permission configuration:  
#  
# Deny requests to certain unsafe ports  
http\_access deny !Safe\_ports

# Deny CONNECT to other than secure SSL ports  
http\_access deny CONNECT !SSL\_ports

# Only allow cachemgr access from localhost  
http\_access allow localhost manager  
http\_access deny manager

# from where browsing should be allowed  
http\_access allow localhost  
http\_access allow broexperts\_network

# And finally deny all other access to this proxy  
http\_access deny all

# 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  
coredump\_dir /var/spool/squid

#  
# Add any of your own refresh\_pattern entries above these.  
#  
refresh\_pattern ^ftp: 1440 20% 10080  
refresh\_pattern ^gopher: 1440 0% 1440  
refresh\_pattern -i (/cgi-bin/|\?) 0 0% 0  
refresh\_pattern . 0 20% 4320  
visible\_hostname pxy.broexperts.com

Now save and exit.

**Step 3:**

Start squid service and make it available on startup.

service squid start  
chkconfig squid on

**Step 4:**

Add firewall rule to allow squid 3128 port.

firewall-cmd –zone=public –add-port=3128/tcp –permanent

Save rules and restart service

firewall-cmd –reload

Done configuration part now time to test browsing pointing squid ip and default port in client browser.

**Step 5:**

Open up firefox browser and go to Tools > Options > Advance tab > Network > Settings > select manual proxy settings radio button and provide squid server IP 192.168.1.100 and port 3128 and check use this use this proxy server for all protocols and then click oK.

Browse **broexperts.com** and see squid access.log file.

tail -f /var/log/squid/access.log

**Sample output:**