Proxy Server

You may not know it (and once you do not know it, it may not bother you), but every time you reach out to a website or connect with anyone online, your online connection gives your computer "address" to the site/person you're connecting with.

Why? So that you the other end knows how to send information (a Web page, email, etc.) back to your computer...to you. That address is your public IP address. IP stands for Internet Protocol.

Without an IP address, you wouldn't be able to do any Internet/online activity and others online wouldn't be able to reach you. It is how you connect to the world.

Where does your IP address come from?

You can thank your Internet Service Provider (AT&T, Comcast, Verizon, etc.) for your IP address at home, as well as for your Internet connection. Your smart device also uses an IP address when you're browsing the web or using an app.

Most people are completely happy with how all of that works.

But there are few realities about public IP addresses that does bother some people:

- Your IP address identifies where you are in the world, sometimes to the street level.
- It can be used by websites to block you from accessing their content.
- It ultimately ties your name and home address to your IP address, because someone is paying for an Internet connection at a specific location.

But there are a few ways you can get around those realities, and one them is to use a proxy service or proxy server (people simply say "proxy.")

Proxy means "substitute."

A proxy lets you go online under a different IP address identity.

You don't change your Internet provider; you simple go online and search for "free proxies" or "list of proxies" and you will get several websites that provide lists of free proxies.

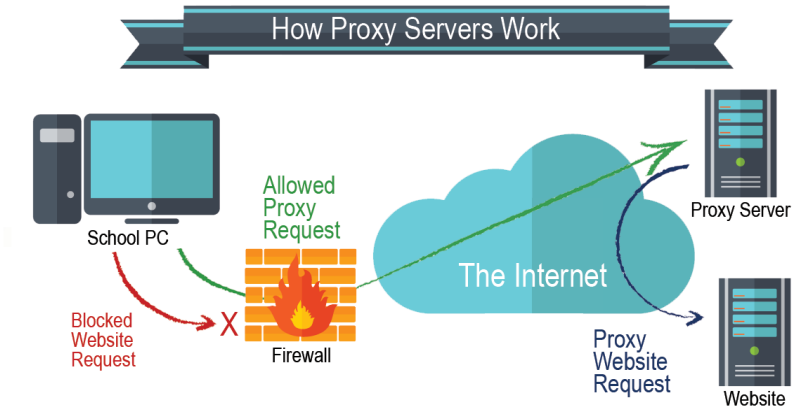
It's really that simple to find proxies, just like you order shoes, movies and airline tickets online. However, it isn't so simple to figure out how to use one without some guidance.

How a proxy operates.

A proxy server is a computer on the web that redirects your web browsing activity. Here's what that means.

- Normally, when you type in a website name (Amazon.com or any other), your Internet Service Provider (ISP) makes the request for you and connects you with the destination—and reveals your real IP address, as mentioned before.
- When you use a proxy your online requests get rerouted.

- While using a proxy, your Internet request goes from your computer to your ISP as usual, but then gets sent to the proxy server, and then to the website/destination. Along the way, the proxy uses the IP address you chose in your setup, masking your real IP address.



Why you might want to use a proxy.

Here why some people turn to using a proxy—and why you might be interested as well.

- A school or local library blocks access to certain websites and a student wants to get around that.
- You want to look at something online that interests you...but you would prefer it couldn't be traced back to your IP address and your location.
- You're traveling abroad and the technology set up in the country you're in prevents you from connecting to a website back home.
- You want to post comments on websites but you do not want your IP address to be identified or your identity tracked down.
- Your employer blocks access to social media or other sites and you'd like to bypass those restrictions.

How to install Squid Proxy Server

Squid proxy server is a free and open-source high performance caching and forwarding HTTP web proxy. It is mostly used for speeding up a web server by caching repeated requests, caching DNS and web lookups for a shared network. It also adds a security policy to filter out unwanted traffics for web or office users.

Step 1 – Install Squid proxy server on Ubuntu

First, log in using the ssh command:

```
ssh user@server-ip-here
ssh vivek@server1.cyberciti.biz
```

Next, update your system using the apt command:

```
sudo apt update
sudo apt upgrade
```

We can search for the squid package as follow:

```
apt show squid
```

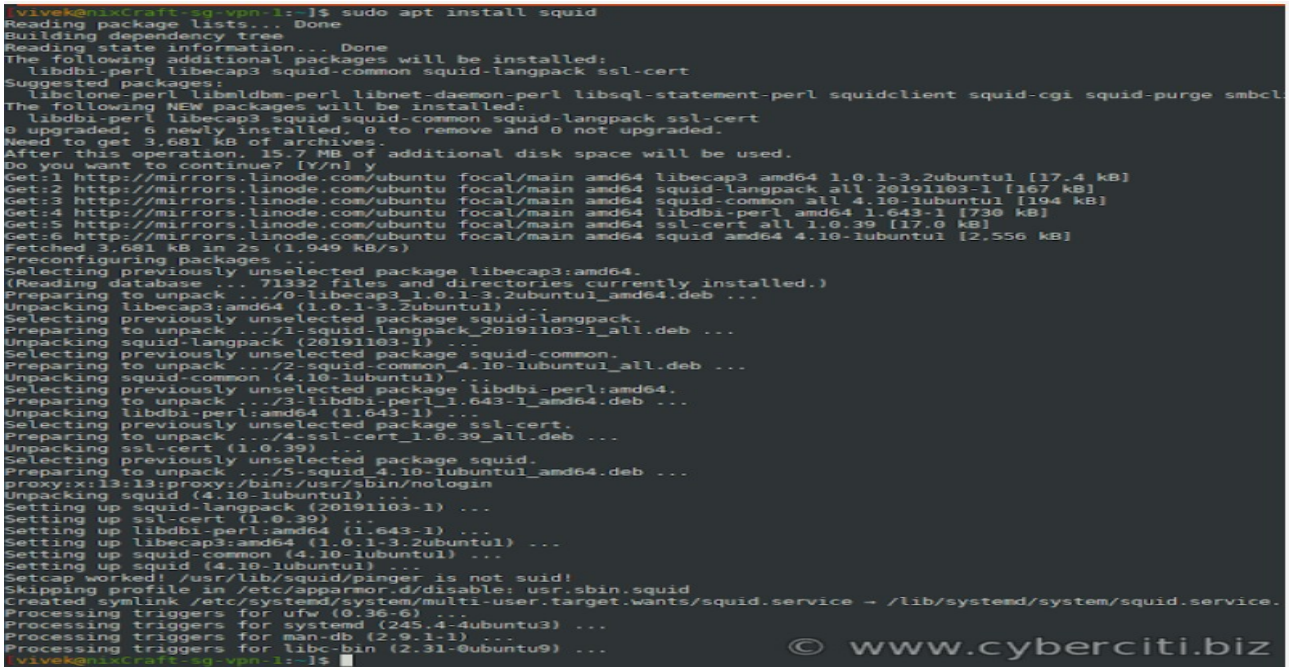
Outputs:

```
Package: squid
Version: 4.10-1ubuntu1
Priority: optional
Section: web
Origin: Ubuntu
Maintainer: Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>
Original-Maintainer: Luigi Gangitano <luigi@debian.org>
Bugs: https://bugs.launchpad.net/ubuntu/+filebug
Installed-Size: 8,792 kB
Provides: squid3
Pre-Depends: adduser
Depends: libc6 (>= 2.29), libcap2 (>= 1:2.10), libcom-err2 (>= 1.43.9),
libdb5.3, libecap3 (>= 1.0.1), libexpat1 (>= 2.0.1), libgcc-s1 (>= 3.0),
libgnutls30 (>= 3.6.6), libgssapi-krb5-2 (>= 1.17), libkrb5-3 (>= 1.10+dfsg~),
libldap-2.4-2 (>= 2.4.7), libltdl7 (>= 2.4.6), libnetfilter-conntrack3 (>=
1.0.7), libnettle7, libpam0g (>= 0.99.7.1), libsasl2-2 (>= 2.1.27+dfsg),
libstdc++6 (>= 9), libxml2 (>= 2.7.4), netbase, logrotate (>= 3.5.4-1), squid-
common (>= 4.10-1ubuntu1), lsb-base, libdbi-perl, ssl-cert
Recommends: libcap2-bin, ca-certificates
Suggests: squidclient, squid-cgi, squid-purge, resolvconf (>= 0.40), smbclient,
ufw, winbind, apparmor
Homepage: http://www.squid-cache.org
Download-Size: 2,556 kB
APT-Sources: http://mirrors.linode.com/ubuntu focal/main amd64 Packages
Description: Full featured Web Proxy cache (HTTP proxy)
 Squid is a high-performance proxy caching server for web clients, supporting
 FTP, gopher, ICY and HTTP data objects.
```

Installing Squid 4

Now that system software up to date, it is time to install the Squid server, enter:

```
sudo apt install squid
```



Step 2 – Configuring Squid server

The squid configuration file is located at /etc/squid/squid.conf and /etc/squid/conf.d/ directory. Let us edit the /etc/squid/squid.conf using a text editor. Make a backup of the original file so that we can go back if something goes wrong using the cp command:

```
sudo cp -v /etc/squid/squid.conf{,.factory}
'/etc/squid/squid.conf' -> '/etc/squid/squid.conf.factory'
```

```
sudo nano /etc/squid/squid.conf
## OR ##
sudo vim /etc/squid/squid.conf
```

Change squid port and listing IP address

By default, squid listens to all IP addresses on all interfaces. The default port is TCP 3128. Find line:

```
http_port 3128
```

Change it as follows or as per your needs:

```
http_port 10.8.0.1:3128
```

Setting up ACL for ports

ACL means an access control scheme, and we can use it to deny or allow access as per our needs. For example, time acl allows you to set up browsing time of day and day of the week for your users. Don't like social media domains? We can block domain such as Facebook and others using the Squid proxy server. There are several different access lists. Let us see some common examples.

Define SSL and safe ports that you would like to allow

```
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
```

Adapt to list your (internal) IP networks from where browsing should be allowed

```
acl localnet src 0.0.0.1-0.255.255.255  # RFC 1122 "this" network (LAN)
acl localnet src 10.0.0.0/8             # RFC 1918 local private network (LAN)
acl localnet src 100.64.0.0/10          # RFC 6598 shared address space (CGN)
acl localnet src 169.254.0.0/16         # RFC 3927 link-local (directly plugged)
machines
acl localnet src 172.16.0.0/12          # RFC 1918 local private network (LAN)
acl localnet src 192.168.0.0/16         # RFC 1918 local private network (LAN)
acl localnet src fc00::/7               # RFC 4193 local private network range
acl localnet src fe80::/10              # RFC 4291 link-local (directly plugged)
machines
```

Define your LAN acl as follows

```
acl mylan src 10.8.0.0/24
```

We can also define other domains that you wish to block

```
acl baddomain1 dstdomain www-bad-guys-domain-name-here
```

Allow or deny access

Use the http_access that allows HTTP clients such as browsers to access the HTTP port. It is the primary access control listL

```
# Block access to all Unsafe ports i.e. only allow Safe_ports defined in acl
above #
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
# Block domains #
http_access deny baddomain1
# only allow cachemgr access from localhost #
http_access allow localhost manager
http_access deny manager
# Allow internet access to localhost and mylan sub/net #
http_access allow localhost
http_access allow mylan
# and finally deny all other access to this proxy server #
http_access deny all
```

Squid Proxy Server Change Outgoing IP Address

Say if you have multiple IP addresses assigned to your server we can change proxy server outgoing IP address as follows:

```
tcp_outgoing_address 139.1.2.3
```

Set cache memory size as per your needs

```
cache_mem 256 MB
```

Force squid to hide client's real IP address

```
forwarded_for delete
via off
forwarded_for off
follow_x_forwarded_for deny all
request_header_access X-Forwarded-For deny all
forwarded_for delete
```

Specify a list of DNS name servers to use

```
dns_nameservers 127.0.0.1 10.8.0.1
```

Squid has many more options.

Verify that config options are valid

To parse and test configuration file, enter:

```
sudo /usr/sbin/squid -k check
echo $?
sudo /usr/sbin/squid -k parse
```

Step 3 - Start/stop/restart Squid

First, turn on Squid service at boot time using the systemctl command:

```
sudo systemctl enable squid.service
```

The syntax is as follows:

Start the Squid server

```
sudo systemctl start squid.service
```

Stop the Squid server

```
sudo systemctl stop squid.service
```

OR

```
sudo squid -k shutdown
```

Restart the Squid server

```
sudo systemctl restart squid.service
```

Find the Squid server status

```
sudo systemctl status squid.service
```

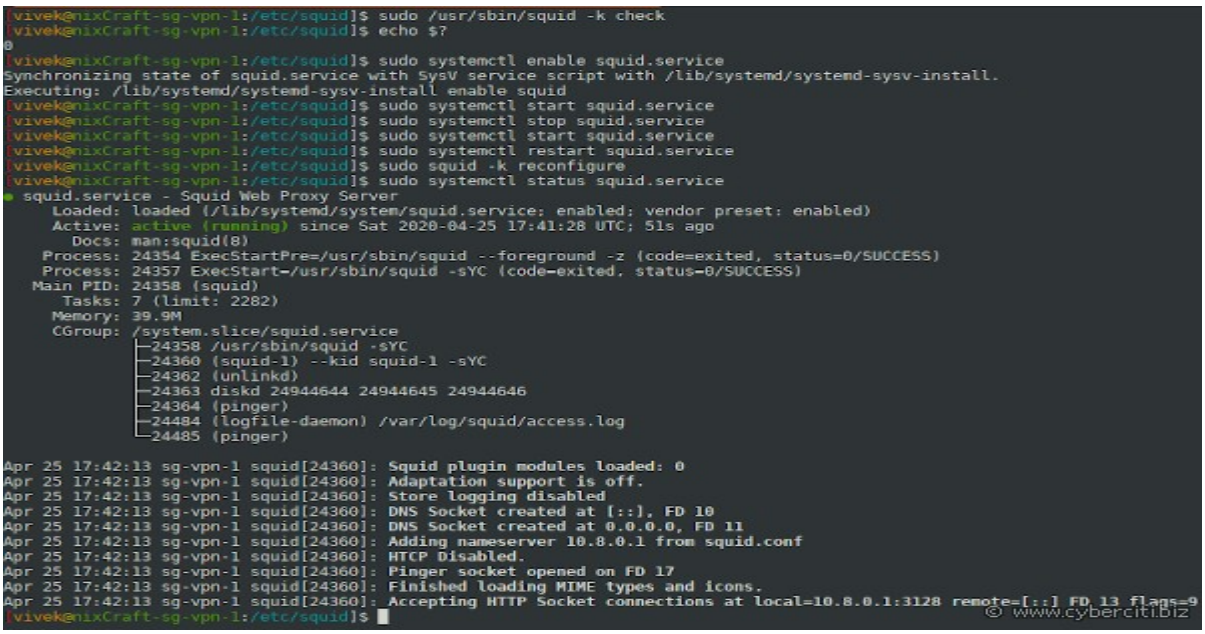
Reload the Squid after config changes gracefully

Whenever you make changes to the squid.conf, reload it as follows:

```
sudo squid -k reconfigure
```

OR

```
sudo systemctl reload squid.service
```



Step 4 - Block domains

Let us block twitter.com and facebook.com:

```
acl socialsite dstdomain .twitter.com
acl socialsite dstdomain .facebook.com
http_access deny socialsite
```

Step 5 - Block URLs using keywords

Say if any url contains keyword such as "`foo`" or "`browse.php?u=`" block it using the url_regex acl:

```
acl urlkeywordsblocks url_regex -i "/etc/squid/blocked-urls-keyword.conf"
http_access deny urlkeywordsblocks
```

Create a file named /etc/squid/blockd-urls-keyword.conf as follows:

```
sudo vim /etc/squid/blocked-urls-keyword.conf
```

Append the urls/keywords:

```
foo
browse.php?u=
```

Step 6 - Block file extensions

We can block unwanted file extensions using the squid proxy too:

```
acl blockedexentions urlpath_regex -i "/etc/squid/blocked-file-externsions.conf"
http_access deny blockedexentions
```

Append the following in /etc/squid/blocked-file-externsions.conf

```
.exec
.mp4
.mp3
```

```
.zip
.pdf
```

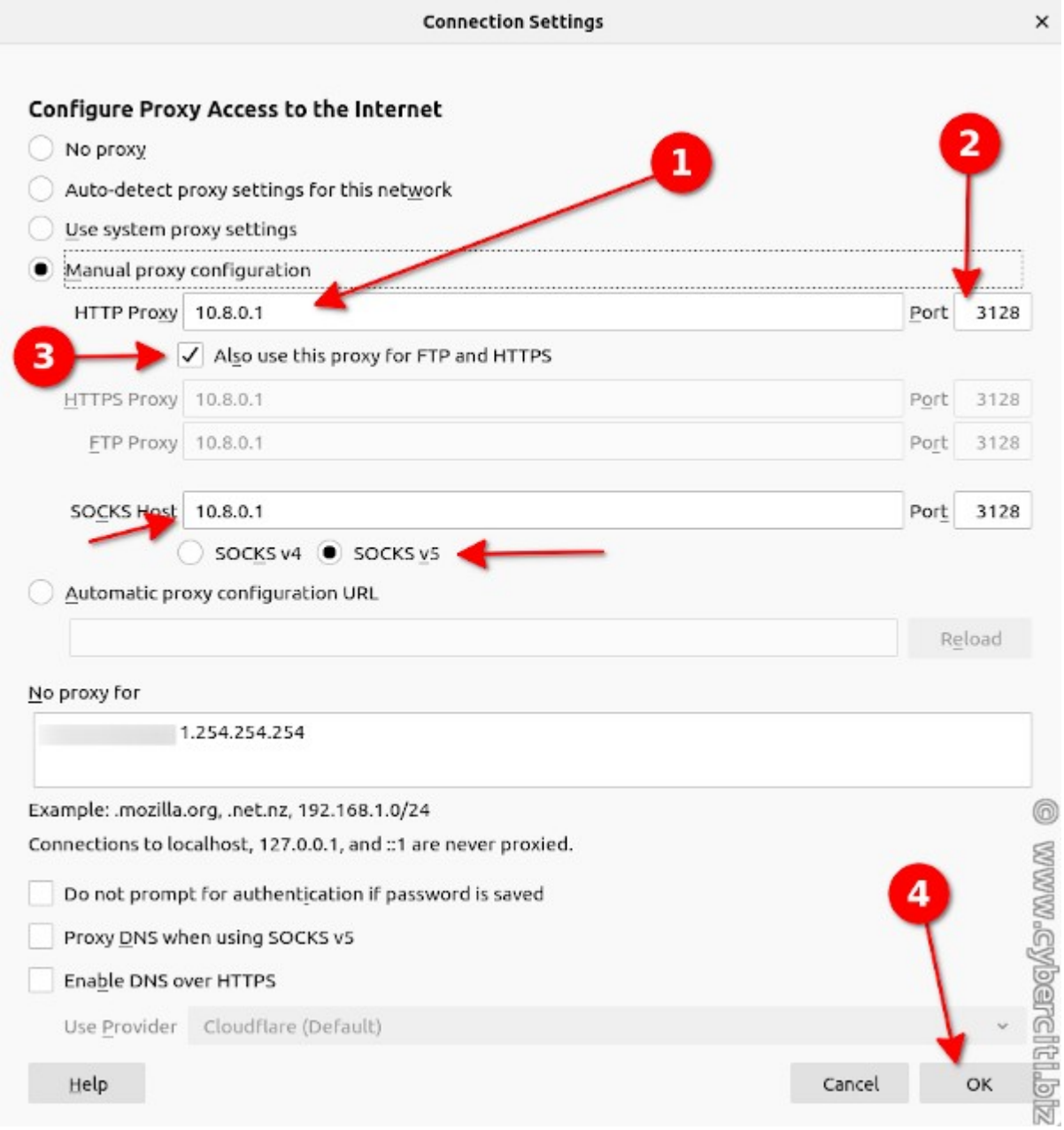
Step 7 - Allow internet access only between 9:00AM and 18:00 during weekdays

```
acl official_hours time M T W H F 09:00-18:00
http_access deny all
http_access allow official_hours
```

Step 8 - Configure web browser

Connection settings to use a proxy can be set in Firefox Preferences as follows:

- Click the **menu** button and select **Preferences**
- In the **General** panel, go to the **Network Settings** section by scrolling down option page.
- Click **Settings...**. The Connection Settings dialog will open and set proxy server address such as 10.8.0.1 and port 3128:



CISCO Packet Tracer Installation:

https://linuxhint.com/install_packet_tracer_ubuntu_1804/