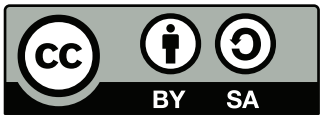
Using SSH for Remote Access

Ubuntu Linux Recipe

By Vernon Van Steenkist

Wednesday 10th July, 2019



Contents

List of Figures

List of Tables

1 Introduction

1.1 Addresses and Ports

In order to understand networking terminology better, let's compare a computer owned by Amazon to the Empire State Building.

Table 1: Computer Networking Analogy

Computer Host Name	Building Name	Comments
www.amazon.com	Empire State Building	
Computer IP Address	**Building Address**	
13.33.154.42	20 W 34th St 10118	
Computer Services	**Building Tenants**	
ssh resides at port 22	Starbucks resides at Suite 100	File /etc/services shows what servers reside at what port

A complete list of ports and what servers reside at these ports can be viewed at https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml

1.2 Introduction to SSH VPN Capabilities

SSH is much more than a secure login shell. With SSH you can easily

- Mount disks on remote computers similar but easier than NFS or CIFS.
- Create a SOCK 5 proxy and route all TCP traffic through that proxy. Some applications that natively support SOCKS 5 proxies are
  - Firefox web browser
  - FileZilla file transfer utility
  - Thunderbird e-mail client
  - ssvnc and RealVNC VNC viewers
  - OpenVPN

Proxychains can be used for many applications that don't natively support SOCKS 5 proxies.

1.3 SOCKS 5 Proxy

To use our building analogy, a SOCKS 5 proxy is like installing a teleporter in a building room. Whoever enters that room is automatically and instantaneously teleported inside your house.

You will learn how to use SSH to create a SOCKS 5 proxy (teleporter) at port 8383 (room number) with the destination of inside your home LAN. You will then learn how to configure applications (Firefox ssVNC etc.) to use the SOCKS 5 proxy created by SSH for all network access as per the figures below.

Figure 1: Access Your Home LAN through SSH SOCKS 5 Proxy

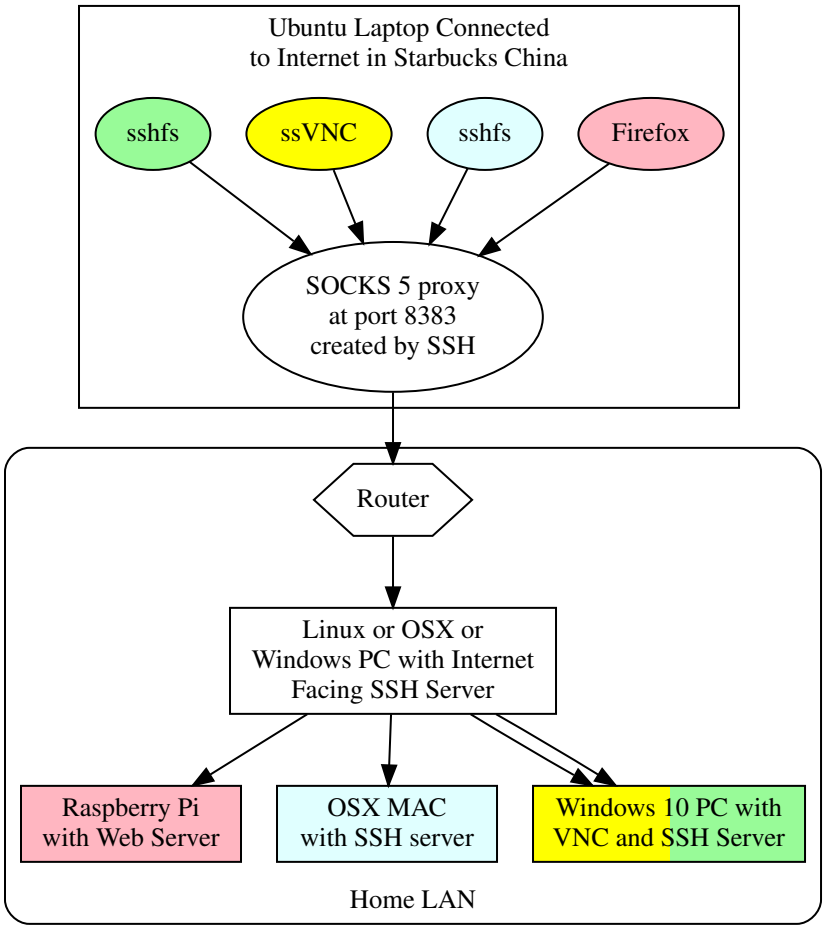
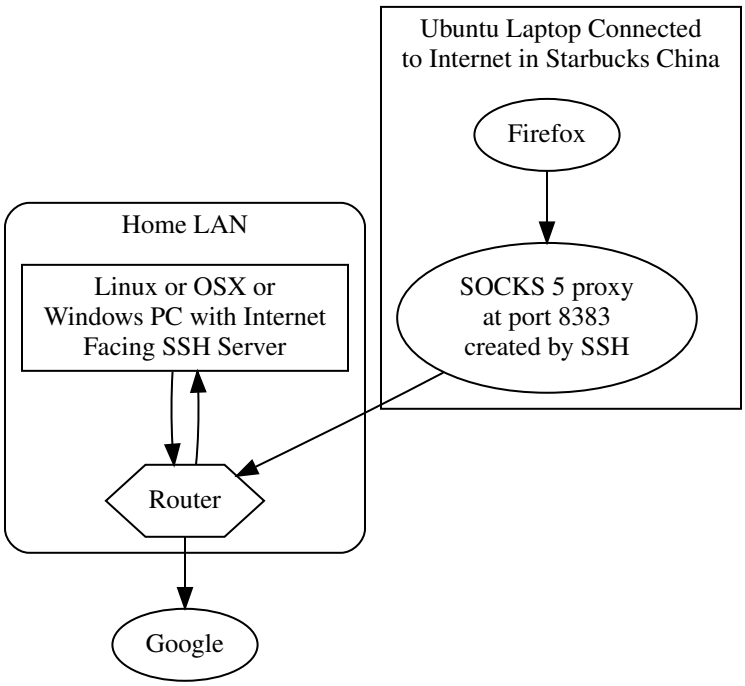


Figure 2: Access Blocked Sites through SSH SOCKS 5 Proxy



Note that Google is blocked in China.

2 Prerequisites

2.1 Remote Use Ubuntu Laptop Necessary Software

The following software is required to be installed on the Ubuntu laptop you plan to use remotely (ex. When you are at Starbucks).

2.1.1 Open a Terminal Window

While connected to your home LAN, open a terminal window by simultaneously pressing the Ctrl Alt T keys.

2.1.2 Install the Network Utility netcat

Copy and paste the following commands into the terminal window and then press the Enter key.

```
sudo apt install netcat-openbsd
```

2.1.3 Install the SSH FUSE File System

Copy and paste the following commands into the terminal window and then press the Enter key.

```
sudo apt install sshfs
```

2.1.4 Install the Proxy Redirection Utility proxychains

Copy and paste the following commands into the terminal window and then press the Enter key.

```
sudo apt install proxychains
```

2.1.5 Install cURL

Copy and paste the following commands into the terminal window and then press the Enter key.

```
sudo apt install curl
```

2.1.6 Install SSL/SSH VNC Viewer (ssVNC)

Copy and paste the following commands into the terminal window and then press the Enter key.

```
sudo apt install ssvnc
```

2.1.7 Install nmap Network Exploration Tool

Copy and paste the following commands into the terminal window and then press the Enter key.

```
sudo apt install nmap
```

2.2 LAN SSH Servers

2.2.1 Find every SSH Server On Your LAN

For Linux computers, open a terminal window by simultaneously pressing the Ctrl Alt T keys. Then copy and paste the following commands into the terminal window and then press the Enter key.

```
nmap -p22 --open $(nmcli -g IP4.ADDRESS con show $(nmcli -g UUID con \
show --active)) | grep "scan report" | cut -d " " -f5 | \
xargs printf "SSH Server at %s\n"
```

The output should look like the below except the IP addresses and host names may be different.

```
SSH Server at tp-link.home
SSH Server at livna.home
SSH Server at raspberrypi.home
SSH Server at latitude-w.home
SSH Server at tv.home
SSH Server at 192.168.0.93
```

Note that if you have a LAN DNS active and the computer is in your DNS, the above command will return host names. Otherwise, an IP address will be returned.

2.2.2 Log In to every SSH Server on your LAN

With your Ubuntu Linux laptop connected to your LAN, make sure you can log in to every computer on your LAN with an SSH server. If the log io was successful, add it to your `~/.ssh/config` file. For example, if Fred has a Windows 10 computer on your LAN at IP addess 192.168.1.103 with a username of bedrock, you would type `ssh bedrock@192.168.1.103` and then press the Enter key.

If you can successfully log in, add Fred's PC to your `~/.ssh/config` file. Copy and paste the following command into a terminal window and then press set Enter key.

```
echo "Host fred-pc
HostName 192.168.1.103
User bedrock
# ProxyCommand nc -x 127.0.0.1:8383 %h %p
#" >> ~/.ssh/config
```

Notes:

- The `Host` name `fred-pc` can be any name that is easy to remember as long as it does not contain any special characters or spaces.
- The `HostName` IP address should be changed to match a PC on your home LAN with an SSH server.

You can now access the PC by simply typing the command `ssh fred-pc` and then pressing the Enter key.

Repeat the above for every computer on your LAN with an SSh server.

2.2.2.1 Home LAN DNS If you are using a home LAN DNS (note that your router probably is a DNS) and you have the same username on all your machines with an SSH server, you don't need to add every computer to your `~/.ssh/config` file. For exanple, if your home LAN domain name is *.home*, copy and paste the following commands into the terminal window and then press the Enter key.

```
echo "Host *.home
# ProxyCommand nc -x 127.0.0.1:8383 %h %p
#" >> ~/.ssh/config
```

SSH will now use your home LAN DNS when typing any host name with a `.home` domain. For example, `ssh raspberrypi.home`.

2.2.3 Create an alias for your Internet Facing SSH Server

While you are connected to your home LAN, copy and paste the following command into a terminal window and then press the Enter key.

```
echo "Host home
HostName $(curl -s ifconfig.me)
User barney
#" >> ~/.ssh/config
```

Note that `User` will more than likely not be `barney` and should match your user name on your Internet facing SSH server. The correct `HostName` will be automatically set by cURL.

When you are done, the contents of your `~/.ssh/config` file should look something like this.

```
Host fred-pc
HostName 192.168.1.103
User bedrock
# ProxyCommand nc -x 127.0.0.1:8383 %h %p
#
Host mypi
HostName 192.168.1.121
User pi
# ProxyCommand nc -x 127.0.0.1:8383 %h %p
#
Host home
HostName 99.84.125.170
User barney
#
```

If you don't have a static IP, your Internet Service Provider may periodically change your Internet IP address. When this occurs, copy and paste the following command into a terminal window and then press the Enter key **when you are connected to your home LAN**.

```
cl=$(awk '/Host home/ {print FNR+1}' ~/.ssh/config); \
sed -i "$cl"'c'"HostName $(curl -s ifconfig.me)" ~/.ssh/config
```

2.3 VNC Server

VNC (Virtual Network Computing) allows you to remotely control another computer graphically. The VNC protocol is low bandwidth since it only sends the graphical changes to the display. Free VNC clients are available for all commonly used platforms including IOS and Android. Install VNC servers on every computer you wish to remote control. Free VNC servers are available for the following platforms.

- Linux - Many. Recommend starting with X11VNC Server.
- Mac OSX - Natively
- Windows - Recommend TightVNC

2.3.1 Install X11VNC Server on an Ubuntu Linux PC

copy and paste the following command into a terminal window and then press the Enter key

```
sudo apt install x11vnc
```

2.3.2 Start and Configure the X11VNC Server

Click on the *X11VNC Server* desktop menu item. It should be in the *Internet* menu. You should see the following screen pop up.

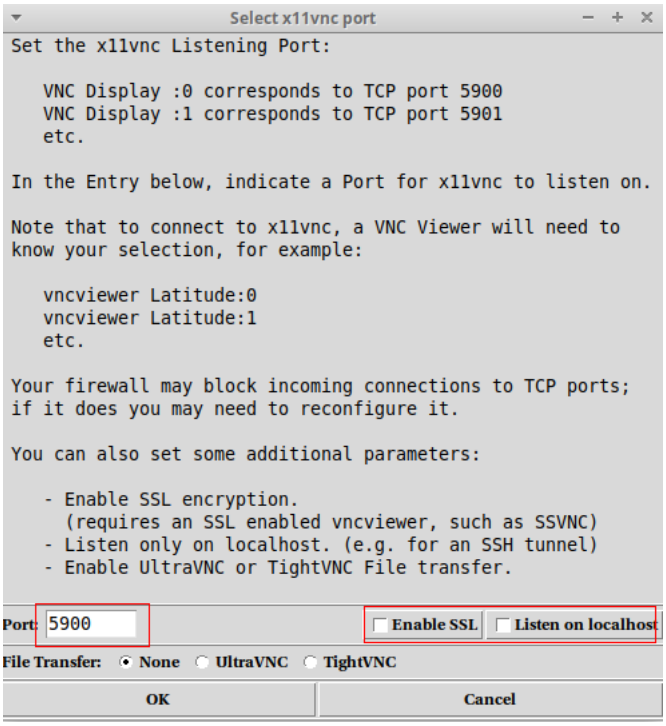


Figure 3: X11VNC Server Initial Screen

Note that *Enable SSL* and *Listen on Localhost* are unticked and should remain so. Click on the *OK* button. The start menu will then pop up shortly.

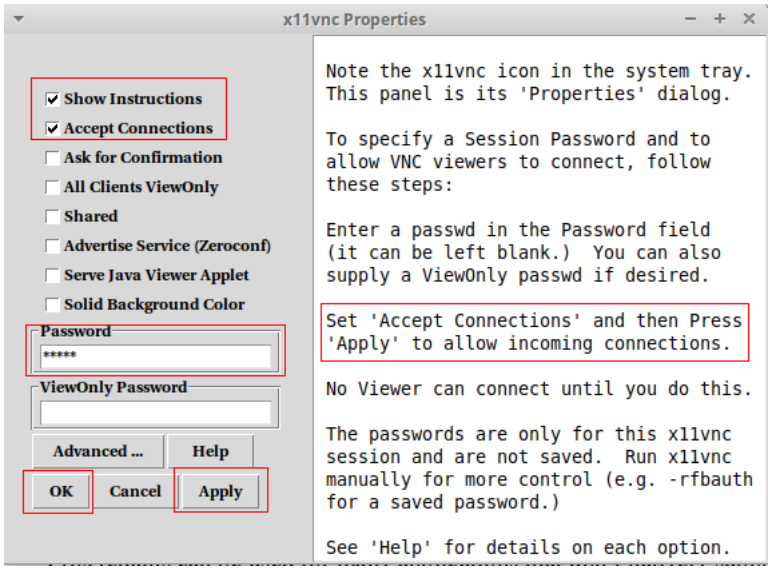


Figure 4: X11VNC Server Startup Screen

Make sure that *Accept Connections* is ticked. Type in a password. This is the password a VNC client will use to remote control your computer. Click *Apply* and then *OK*

2.3.3 Test the VNC Server

Probably the easiest way to test X11VNC Server is to install *VNC Viewer* by *RealVNC* on your IOS or Android device. *VNC Viewer* is free on all platforms. Enter the IP adddress of your Ububru computer and the password for your X11VNC Server into *VNC Viewer*. Ignore any warning about an insecure connection.

2.4 SSH Server Facing the Internet

An SSH server on your home LAN accessible to the Internet. SSH servers are available for the following operating systems.

- Linux - Natively
- Mac OSX - Natively
- Android - through Termux
- Windows 10 - Natively. Through Cygwin for older versions of Windows.

3 Remote Location Ubuntu Laptop Configuration and Usage

Once you are at a remote location, ex. Starbucks and connected to the Internet, you will need to set up your Ubuntu Laptop.

3.1 Redirect SSH Traffic through your SOCKS 5 Proxy

Open a terminal window by simultaneously pressing the Ctrl Alt T keys. Copy and paste the following commands into the Terminal window and then press the Enter key.

```
sed -i 's/# ProxyCommand/ProxyCommand/g' ~/.ssh/config
```

The above command will tell SSH or sshfs to re-direct any traffic for any `Host` defined in your `~/.ssh/config` file through your SOCKS 5 proxy.

Note than when your are back home, you will no longer want to re-direct SSH traffic through SOCKS 5 proxy. **When you are back home, copy and past the following commands in a Terminal Window** and then press the Enter key.

```
sed -i 's/ProxyCommand/# ProxyCommand/g' ~/.ssh/config
```

3.2 Create a SOCKS 5 Proxy

If you have a Linux or Mac OSX Internet facing SSH server on your home LAN, copy and paste the following command into the Terminal window and then press the Enter key.

```
ssh -D 8383 home "while date; do sleep 15; done"
```

You should see the current date and time update every 15 seconds in your terminal window.

Some routers/firewalls will close down connections if they remain idle for a certain period of time. The `while date; do sleep 15; done` part of the command generates traffic every 15 seconds between your remote Ubuntu laptop and your home LAN ensuring that your connection remains open.

The SOCKS 5 proxy can be killed by pressing the Ctrl C keys simultaneously.

3.3 Mount Your Home LAN PC's Disk Drives

Open another terminal window by simultaneously pressing the Ctrl Alt T keys. You can easily mount the disk drives of every `Host` in your `~/.ssh/config` file. We will use `Host fred-pc` as am example.

3.3.1 Create a Mount Point

Create an empty directory by copying and pasting the following command into the Terminal window and then pressing the Enter key.

```
mkdir ~/fred-pc
```

3.3.2 Mount the Disk of a Computer on Your Home LAN

Copy and paste the following command into the Terminal window and then press the Enter key.

```
sshfs fredpc: ~/fred-pc
```

Now, every time you enter the `fred-pc` directory, you will be accessing the files on *fred-pc* which is on your home LAN. Just like on your local disk, you can read, write, execute and delete these files so be careful.

You can repeat the above steps for each `Host` in your `~/.ssh/config` file.

If you no longer want the `fred-pc` directory to be associated with files on *fred-pc*, copy and paste the following command into the Terminal window and press the Enter key.

```
fusermount -u ~/fred-pc
```

3.4 Configure Firefox to use the SOCKS 5 proxy

1. Open Firefox
2. Copy and past *about:preferences#general* into the Firefox URL window and press the Enter key.
3. Scroll down to *Network Settings* and then click on the *Settings* button.
4. Fill out the pop-up menu as per the figures below.

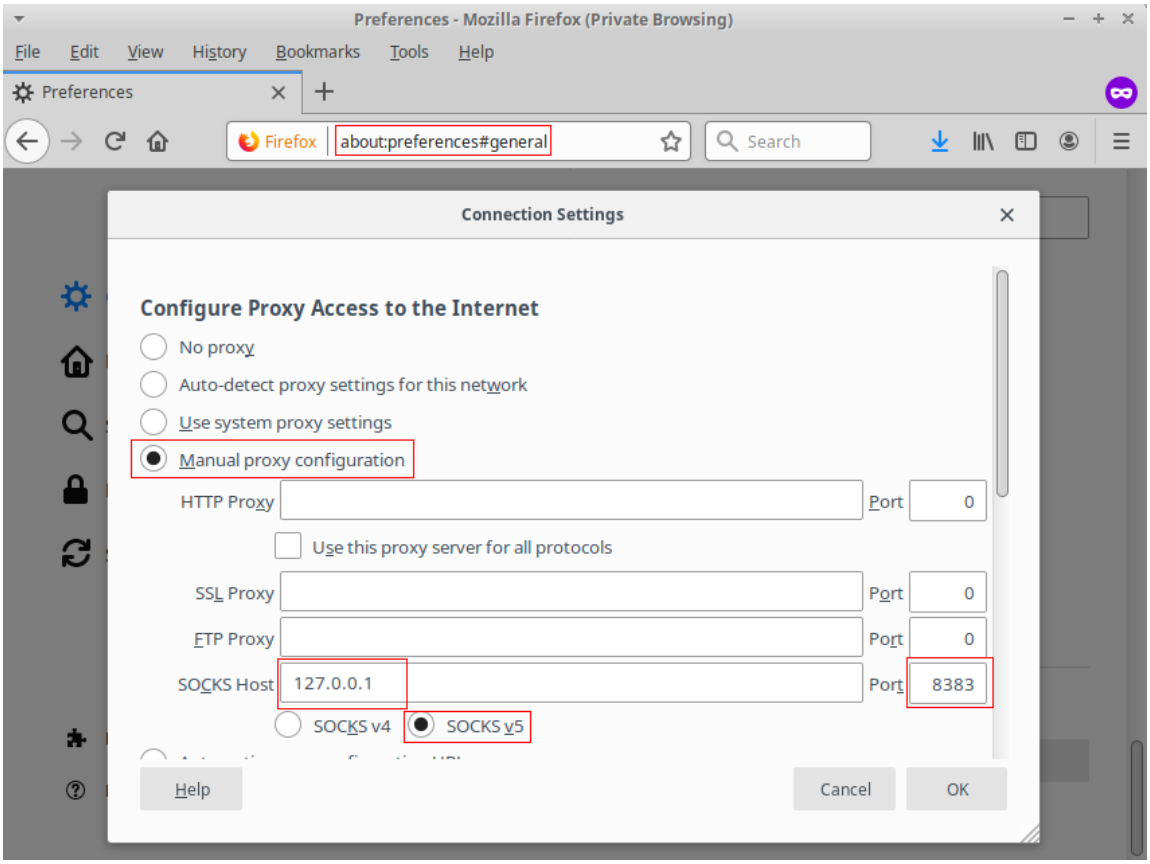


Figure 5: SOCKS 5 Proxy Firefox Configuration

Scroll to the bottom of the *Connection Setting* window and make sure that *Proxy DNS when using SOCKS v5* is ticked as per the figure below. Then click on the *OK* button.

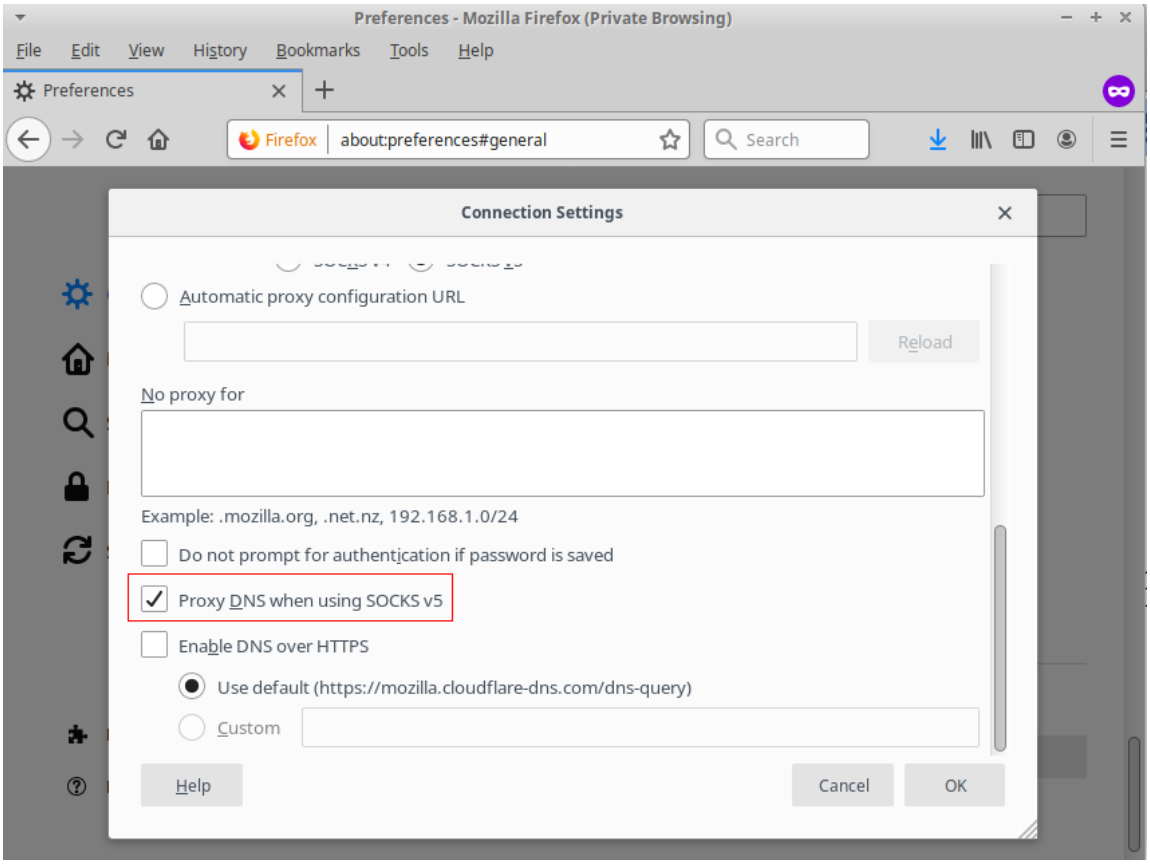


Figure 6: Firefox Use Proxy DNS

When you are re-connected to you home LAN or other times when you no longer want to route Firefox through your SOCKS 5 proxy, tick the *No proxy* button as per the figure below. Then click on the *OK* button.

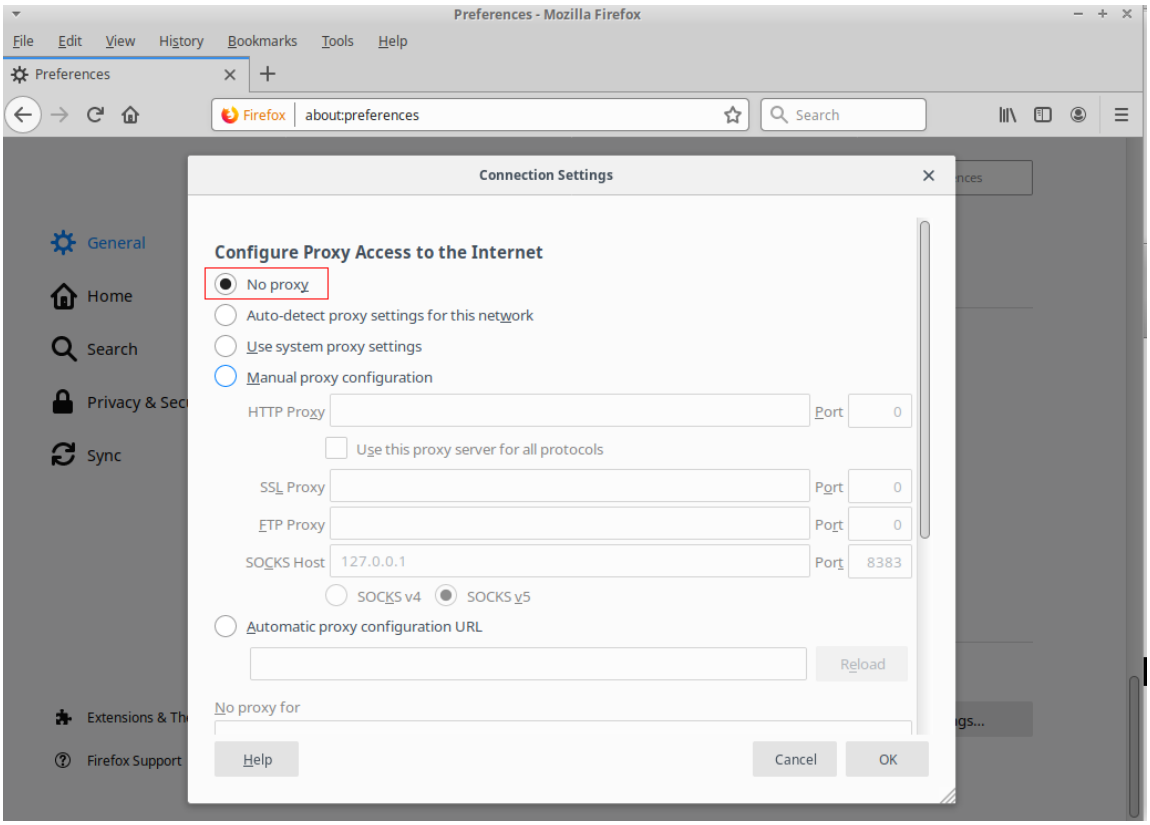


Figure 7: No Proxy Firefox Configuration

Note that Firefox remembers all of your proxy settings. Now you can easily switch between using and not using your SOCKS 5 proxy by simply ticking *Manual proxy configuration* or the *No proxy* button.

3.5 Configure SSL/SSH VNC Viewer to use the SOCKS 5 proxy

Let's assume you have a computer running a VNC server at IP address 192.168.1.103 on your home LAN. You can remote control this computer by clicking on the *SSL/SSH VNC Viewer* desktop menu item. It should be in the *Internet* menu. Fill out the menu as per the figure below.

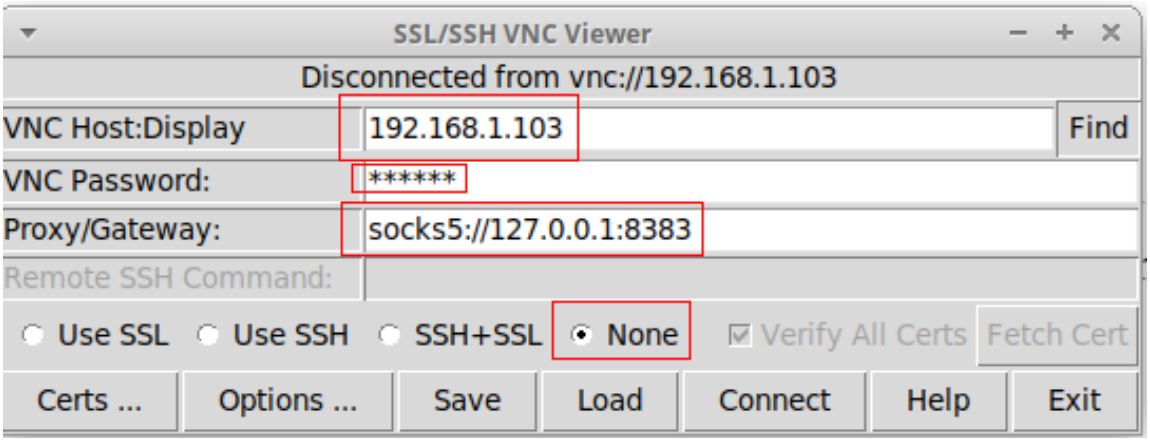


Figure 8: SOCKS 5 Proxy Configuration for SSL/SSH VNC Viewer

Note that *VNC Password* is the password you entered when you started your VNC server on 192.168.1.103 and may be different from your login password for that computer.

When you are finished, click on the *Connect* button. Once you are connected, the *SSL/SSH VNC Viewer* pop-up control menu can be invoked by pressing the F8 key.

3.6 Applications that Don't Natively support SOCKS 5

Although there are other applications like FileZilla and Thunderbird which do support SOCKS 5, you can pre-pend the command `proxychains` for applications that do not. First, ensure that the end of your `/etc/proxychains.conf` looks like below.

```
# ProxyList format
#       type  host  port [user pass]
#       (values separated by 'tab' or 'blank')
#
#
#        Examples:
#
#               socks5  192.168.67.78   1080    lamer   secret
#               http    192.168.89.3    8080    justu   hidden
#               socks4  192.168.1.49    1080
#               http    192.168.39.93   8080
#
#
#       proxy types: http, socks4, socks5
#        ( auth types supported: "basic"-http  "user/pass"-socks )
#
[ProxyList]
# add proxy here ...
# meanwile
# defaults set to "tor"
# socks4        127.0.0.1 9050
socks5 127.0.0.1 8383
```

The command line *FTP* application does not natively support SOCKS 5 proxies. However, you can now route *FTP* through your SOCKS 5 proxy by typing the following command in a Terminal window and then press the Enter key.

```
proxychains ftp 192.168.0.103
```

Congratulations, you are now the ultimate road warrior!