



Linux Applications

How to Tunnel Web Traffic Through SSH for Secure Browsing

5 months ago • by Prateek Jangid

Nowadays, an uncountable number of cyber attacks, scams, and data theft occur every single day. This makes it necessary for users to look for ways to secure their data. After all, it is better to take precautions than to experience a guilt trip. Fortunately, SSH offers tunneling, which channels internet traffic to your local system via a remote system.

Meanwhile, this transmission encrypts incoming and outgoing network traffic on your local Linux device, ensuring the system's security. Many users are still unaware of how to create an SSH tunnel. So, if you are one of them, don't worry; we will explain how to tunnel web traffic through SSH for secure browsing without hassles.

How to Tunnel Web Traffic Through SSH for Secure Browsing

Before moving to the tunneling process, please ensure you follow the below prerequisites:

1. Two Linux devices (local and remote).
2. Both devices should have SSH installed.

To tunnel the web traffic through SSH, you must first create an SSH tunnel on your local device using the following command:

```
ssh -D 8080 -C -N user@remote_server  
prateek@prateek:~$ ssh -D 8080 -C -N prateek@domain.com
```

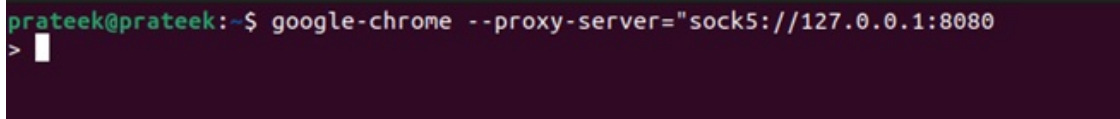
Here:

1. the '-D' option lets you specify the local port number for creating a dynamic SOCKS (SSH encrypted) tunnel.
2. Please replace 8080 with your desired port number.

3. The '-C' option enables data compression to enhance performance during large data transfers.
4. The '-N' option specifies that the system should set up the tunnel and not allow the execution of remote commands.

When run, the above command should open an SSH tunnel. To use it for browsing purposes, you must configure your web browser to use a SOCKS proxy. This configuration setting can be different for different browsers. For example, in the case of Google Chrome, you can open a terminal tab and run:

```
google-chrome --proxy-server="socks5://127.0.0.1:8080"
```



This command will open Chrome with the SOCKS5 proxy. You should replace 127.0.0.1 with your IP address on the local host and 8080 with the port you specified in the earlier command. Finally, you can test whether the connection is successful by entering the following URL in your browser's URL field:

```
https://127.01.80.1001.com
```

Alternatively, you can cross-verify the IP addresses of your local and remote devices. If the tunnel connection is established successfully, both the IPs will match.

A Quick Wrap-up

SSH tunneling provides a secure means of browsing the Internet, ensuring your data is protected from threats or third-party interference. This guide briefly explains how to tunnel web traffic through SSH for secure browsing. You should cautiously set up the SOCKS proxy on your browser; otherwise, the SSH tunnel will not work.

ABOUT THE AUTHOR



Prateek Jangid

[View all posts](#)

RELATED LINUX HINT POSTS

How to SSH Into EC2 Instance

How to SSH Into Docker Container

**HOW TO TUNNEL WEB TRAFFIC
THROUGH SSH FOR SECURE
BROWSING**

How To Add SSH Key to GitHub

**How to Setup and Use Sshfs in
Linux**

**How to Use SSH to Access a
Remote Server in Linux**

How to Log Out of SSH

Linux Hint LLC, editor@linuxhint.com
1210 Kelly Park Circle, Morgan Hill, CA
95037

[Privacy Policy](#) and [Terms of Use](#)
