# COMPUTER NETWORK SECURITY LABORATORY

| | | |
|---|---|---|
| NAME : PREM SAGAR J S | SRN : PES1UG20CS825 | SEC : H |

## Firewall Evasion Lab

### Task 0 : Get Familiar with the Lab Setup

Lab Environment Setup

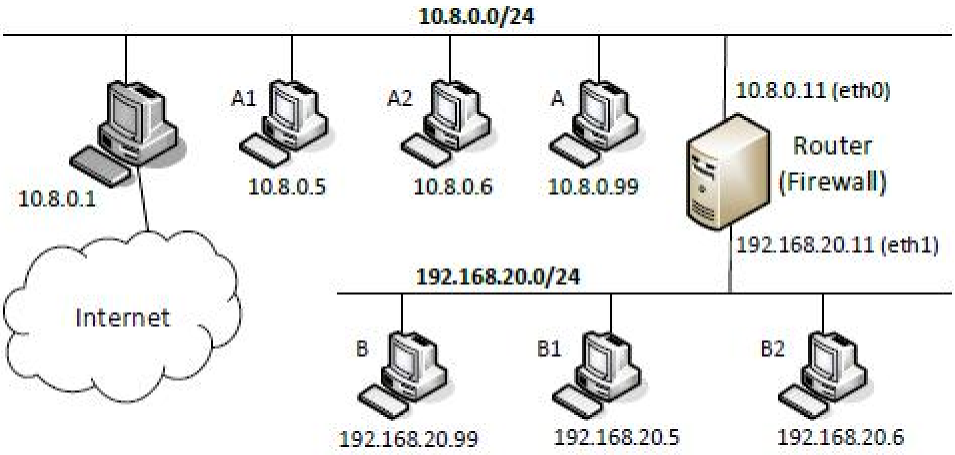


Figure 1: Network setup

.

Router configuration :-

**Lab task :** Please block two more websites and add the firewall rules to the setup files. The choice of websites are up to you. Keep in mind that most popular websites have multiple IP addresses that can change from time to time. After adding the rules, start the containers, and verify that all the ingress and egress firewall rules are working as expected.

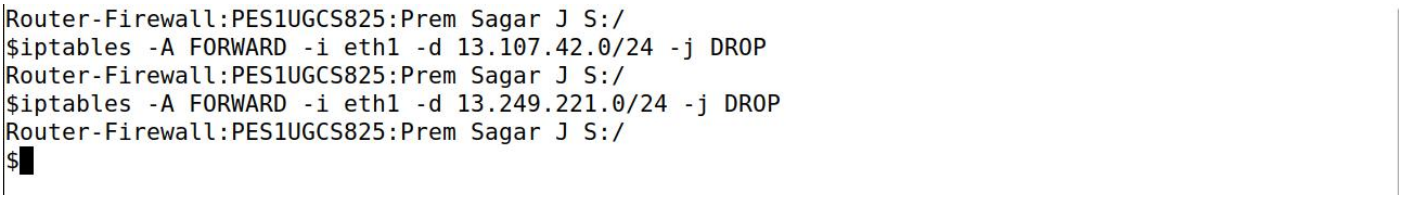
On the router-firewall container:

```
# iptables -A FORWARD -i eth1 -d 13.107.42.0/24 -j DROP
```

This IP address was for www.linkedin.com

```
# iptables -A FORWARD -i eth1 -d 13.249.221.0/24 -j DROP
```

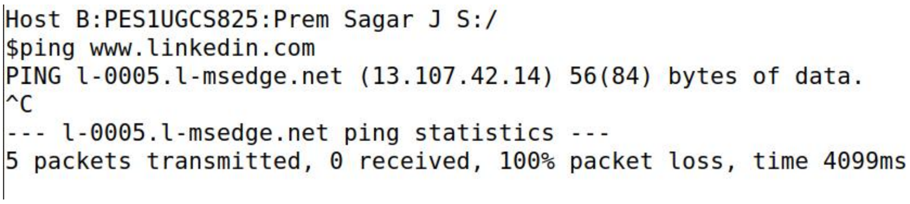
This IP address was for www.miniclip.com



```
Router-Firewall:PES1UGCS825:Prem Sagar J S:/
$iptables -A FORWARD -i eth1 -d 13.107.42.0/24 -j DROP
Router-Firewall:PES1UGCS825:Prem Sagar J S:/
$iptables -A FORWARD -i eth1 -d 13.249.221.0/24 -j DROP
Router-Firewall:PES1UGCS825:Prem Sagar J S:/
$
```

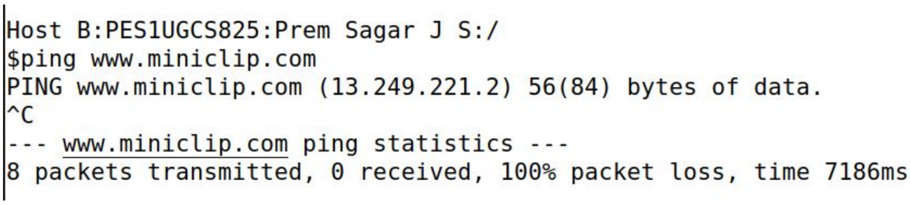
To verify that the websites have been blocked,ping them from any machine in the internal network

# ping www.linkedin.com



```
Host B:PES1UGCS825:Prem Sagar J S:/
$ping www.linkedin.com
PING l-0005.l-msedge.net (13.107.42.14) 56(84) bytes of data.
^C
--- l-0005.l-msedge.net ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4099ms
```

# ping www.miniclip.com



```
Host B:PES1UGCS825:Prem Sagar J S:/
$ping www.miniclip.com
PING www.miniclip.com (13.249.221.2) 56(84) bytes of data.
^C
--- www.miniclip.com ping statistics ---
8 packets transmitted, 0 received, 100% packet loss, time 7186ms
```

Task 1 : Static Port Forwarding

Lab task : Please use static port forwarding to create a tunnel between the external network and the internal network, so we can telnet into the server on B. Please demonstrate that you can do such telnet from hosts A, A1 and A2.

**(1) How many TCP connections are involved in this entire process. You should run wireshark or tcpdump to capture the network traffic, and then point out all the involved TCP connections from the captured traffic.**

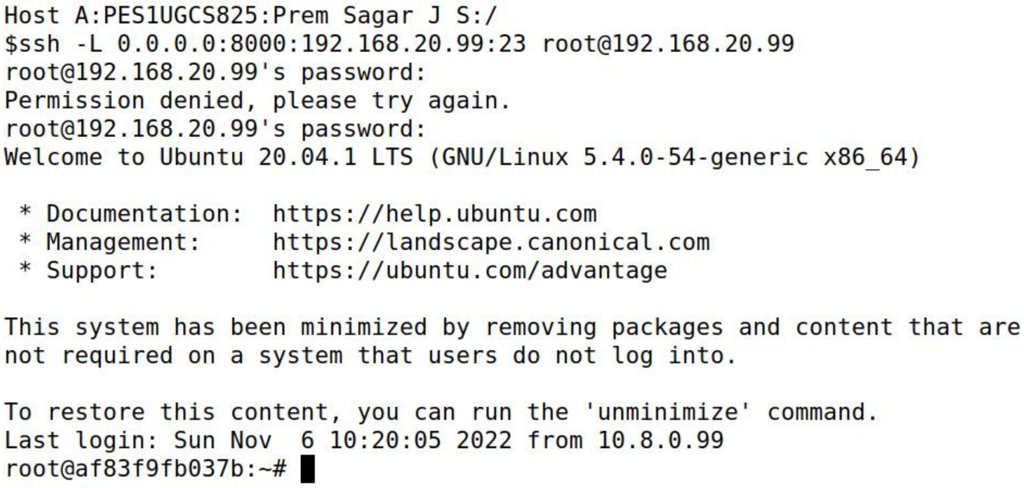
Totally 3 TCP Connections were involved in this entire process,One connection on container A for local forwarding, one on the 192.168.20.99 machine
For ssh to the server B on the internal network and another one is the client machine to intermediate that is root@192.168.20.99.

**(2) Why can this tunnel successfully help users evade the firewall rule specified in the lab setup?**

Container A is on the external network,a direct access to the server machine on the internal network is not permitted by the firewall, by using
Ssh tunneling we are using ssh connection from our client machine to the another machine internal machine then we contacting with the server.

Run the below command on container A:

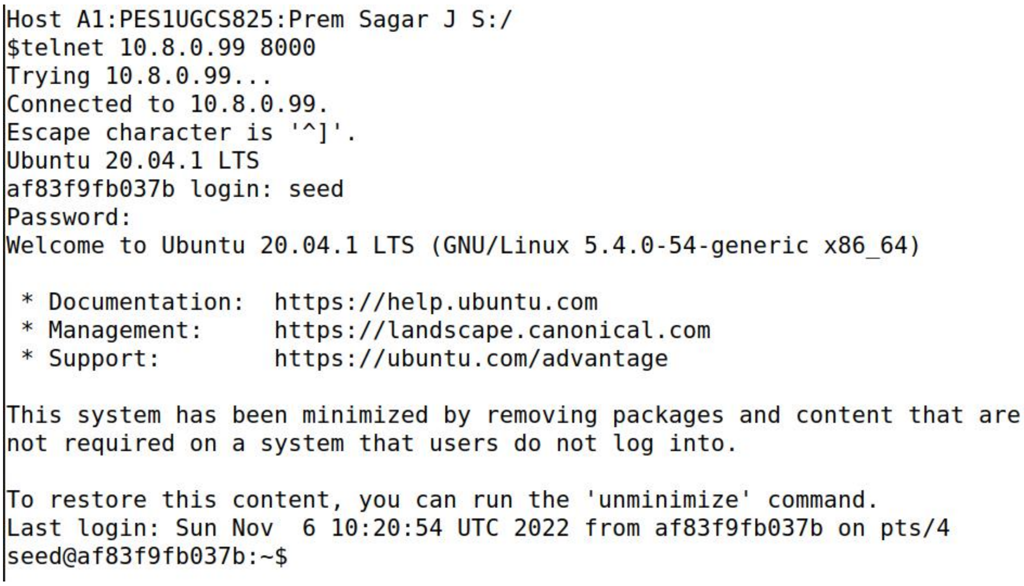
# ssh -L 0.0.0.0:8000:192.168.20.99:23 root@192.168.20.99



```
Host A:PES1UGCS825:Prem Sagar J S:/
$ssh -L 0.0.0.0:8000:192.168.20.99:23 root@192.168.20.99
root@192.168.20.99's password:
Permission denied, please try again.
root@192.168.20.99's password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Sun Nov  6 10:20:05 2022 from 10.8.0.99
root@af83f9fb037b:~# 
```

Run the below command on container A1:

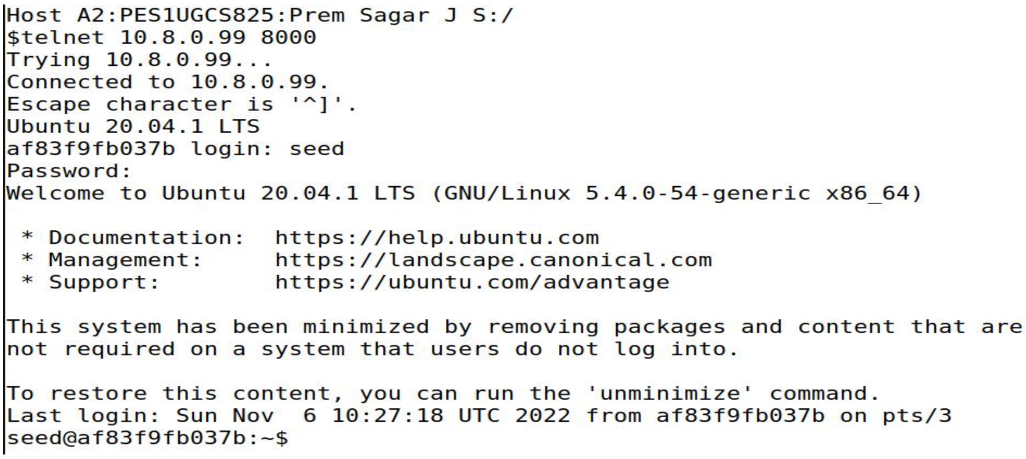
# telnet 10.8.0.99 8000



```
Host A1:PES1UGCS825:Prem Sagar J S:/
$telnet 10.8.0.99 8000
Trying 10.8.0.99...
Connected to 10.8.0.99.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
af83f9fb037b login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Sun Nov  6 10:20:54 UTC 2022 from af83f9fb037b on pts/4
seed@af83f9fb037b:~$
```

Run the below command on container A2:

# telnet 10.8.0.99 8000

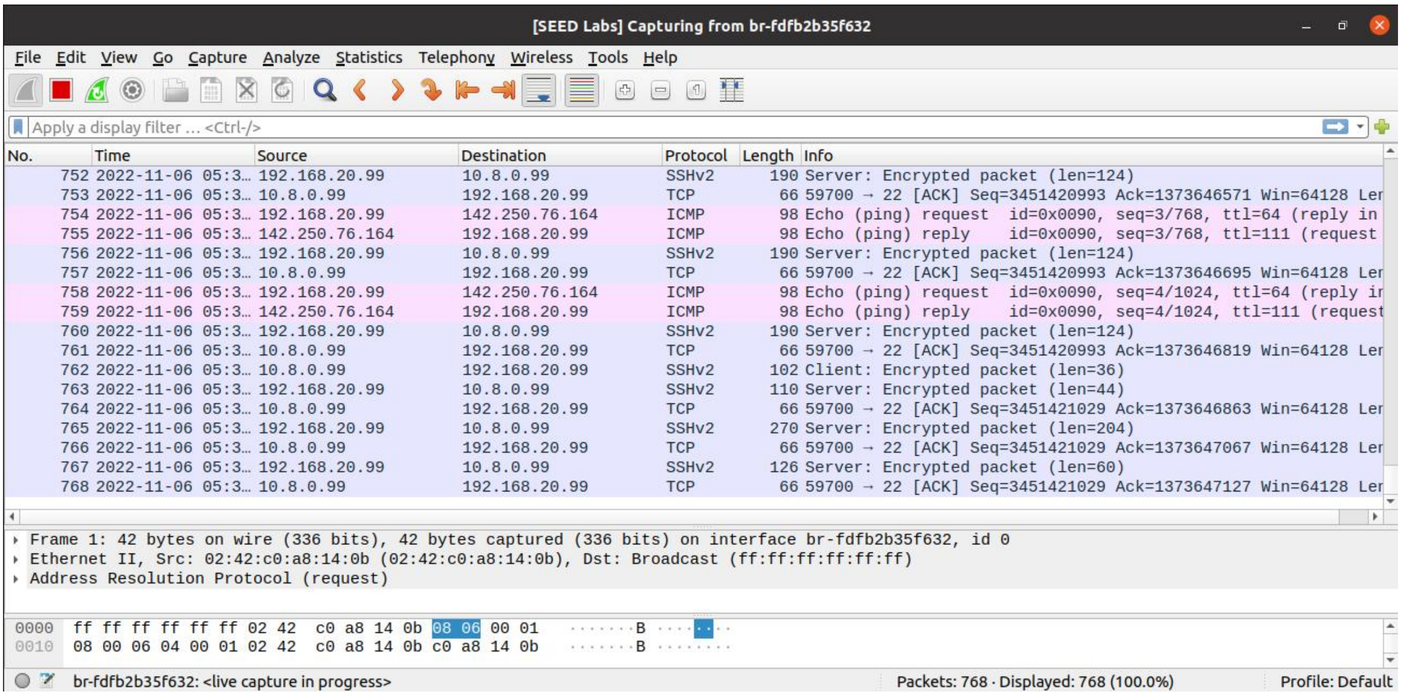


```
Host A2:PES1UGCS825:Prem Sagar J S:/
$telnet 10.8.0.99 8000
Trying 10.8.0.99...
Connected to 10.8.0.99.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
af83f9fb037b login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Sun Nov  6 10:27:18 UTC 2022 from af83f9fb037b on pts/3
seed@af83f9fb037b:~$
```

Pinging www.google.com on Host A2

```
seed@af83f9fb037b:~$ ping www.google.com
PING www.google.com (142.250.76.164) 56(84) bytes of data.
64 bytes from bom12s09-in-f4.1e100.net (142.250.76.164): icmp_seq=1 ttl=111 time=161 ms
64 bytes from bom12s09-in-f4.1e100.net (142.250.76.164): icmp_seq=2 ttl=111 time=85.5 ms
64 bytes from bom12s09-in-f4.1e100.net (142.250.76.164): icmp_seq=3 ttl=111 time=89.3 ms
64 bytes from bom12s09-in-f4.1e100.net (142.250.76.164): icmp_seq=4 ttl=111 time=92.6 ms
�^C
--- www.google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3010ms
rtt min/avg/max/mdev = 85.483/107.216/161.441/31.407 ms
seed@af83f9fb037b:~$
```

Wireshark Output :


[SEED Labs] Capturing from br-fdfb2b35f632
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time               Source           Destination      Protocol Length Info
 752 2022-11-06 05:3… 192.168.20.99    10.8.0.99        SSHv2    190 Server: Encrypted packet (len=124)
 753 2022-11-06 05:3… 10.8.0.99        192.168.20.99    TCP       66 59700 → 22 [ACK] Seq=3451420993 Ack=1373646571 Win=64128 Ler
 754 2022-11-06 05:3… 192.168.20.99    142.250.76.164   ICMP      98 Echo (ping) request  id=0x0090, seq=3/768, ttl=64 (reply in
 755 2022-11-06 05:3… 142.250.76.164   192.168.20.99    ICMP      98 Echo (ping) reply    id=0x0090, seq=3/768, ttl=111 (request
 756 2022-11-06 05:3… 192.168.20.99    10.8.0.99        SSHv2    190 Server: Encrypted packet (len=124)
 757 2022-11-06 05:3… 10.8.0.99        192.168.20.99    TCP       66 59700 → 22 [ACK] Seq=3451420993 Ack=1373646695 Win=64128 Ler
 758 2022-11-06 05:3… 192.168.20.99    142.250.76.164   ICMP      98 Echo (ping) request  id=0x0090, seq=4/1024, ttl=64 (reply ir
 759 2022-11-06 05:3… 142.250.76.164   192.168.20.99    ICMP      98 Echo (ping) reply    id=0x0090, seq=4/1024, ttl=111 (request
 760 2022-11-06 05:3… 192.168.20.99    10.8.0.99        SSHv2    190 Server: Encrypted packet (len=124)
 761 2022-11-06 05:3… 10.8.0.99        192.168.20.99    TCP       66 59700 → 22 [ACK] Seq=3451420993 Ack=1373646819 Win=64128 Ler
 762 2022-11-06 05:3… 10.8.0.99        192.168.20.99    SSHv2    102 Client: Encrypted packet (len=36)
 763 2022-11-06 05:3… 192.168.20.99    10.8.0.99        SSHv2    110 Server: Encrypted packet (len=44)
 764 2022-11-06 05:3… 10.8.0.99        192.168.20.99    TCP       66 59700 → 22 [ACK] Seq=3451421029 Ack=1373646863 Win=64128 Ler
 765 2022-11-06 05:3… 192.168.20.99    10.8.0.99        SSHv2    270 Server: Encrypted packet (len=204)
 766 2022-11-06 05:3… 10.8.0.99        192.168.20.99    TCP       66 59700 → 22 [ACK] Seq=3451421029 Ack=1373647067 Win=64128 Ler
 767 2022-11-06 05:3… 192.168.20.99    10.8.0.99        SSHv2    126 Server: Encrypted packet (len=60)
 768 2022-11-06 05:3… 10.8.0.99        192.168.20.99    TCP       66 59700 → 22 [ACK] Seq=3451421029 Ack=1373647127 Win=64128 Ler

▸ Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface br-fdfb2b35f632, id 0
▸ Ethernet II, Src: 02:42:c0:a8:14:0b (02:42:c0:a8:14:0b), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▸ Address Resolution Protocol (request)

0000  ff ff ff ff ff ff 02 42  c0 a8 14 0b 08 06 00 01   ·······B ········
0010  08 00 06 04 00 01 02 42  c0 a8 14 0b c0 a8 14 0b   ·······B ········

br-fdfb2b35f632: <live capture in progress>        Packets: 768 · Displayed: 768 (100.0%)        Profile: Default
```

## Task 2: Dynamic Port Forwarding

If we want to forward data to multiple destinations, we need to set up multiple tunnels.

For example, using port forwarding, we can successfully visit the blocked example.com website, but what if the firewall blocks many other sites, how do we avoid tediously establishing an SSH tunnel for each site?

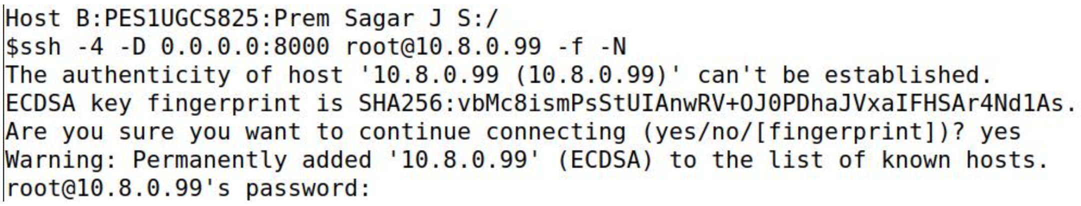
We can use dynamic port forwarding to solve this problem.

### Task 2.1: Setting Up Dynamic Port Forwarding

We can use ssh to create a dynamic port-forwarding tunnel between B and A.

Run in container B to set up the ssh shell with dynamic port forwarding enabled:

```
# ssh -4 -D 0.0.0.0:8000 root@10.8.0.99 -f -N
```



```
Host B:PES1UGCS825:Prem Sagar J S:/
$ssh -4 -D 0.0.0.0:8000 root@10.8.0.99 -f -N
The authenticity of host '10.8.0.99 (10.8.0.99)' can't be established.
ECDSA key fingerprint is SHA256:vbMc8ismPsStUIAnwRV+OJ0PDhaJVxaIFHSAr4Nd1As.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.8.0.99' (ECDSA) to the list of known hosts.
root@10.8.0.99's password:
```

Lab task. Please demonstrate that you can visit all the blocked websites using curl from hosts B, B1,
and B2 on the internal network. Please also answer the following questions:

(1) Which computer establishes the actual connection with the intended web server?

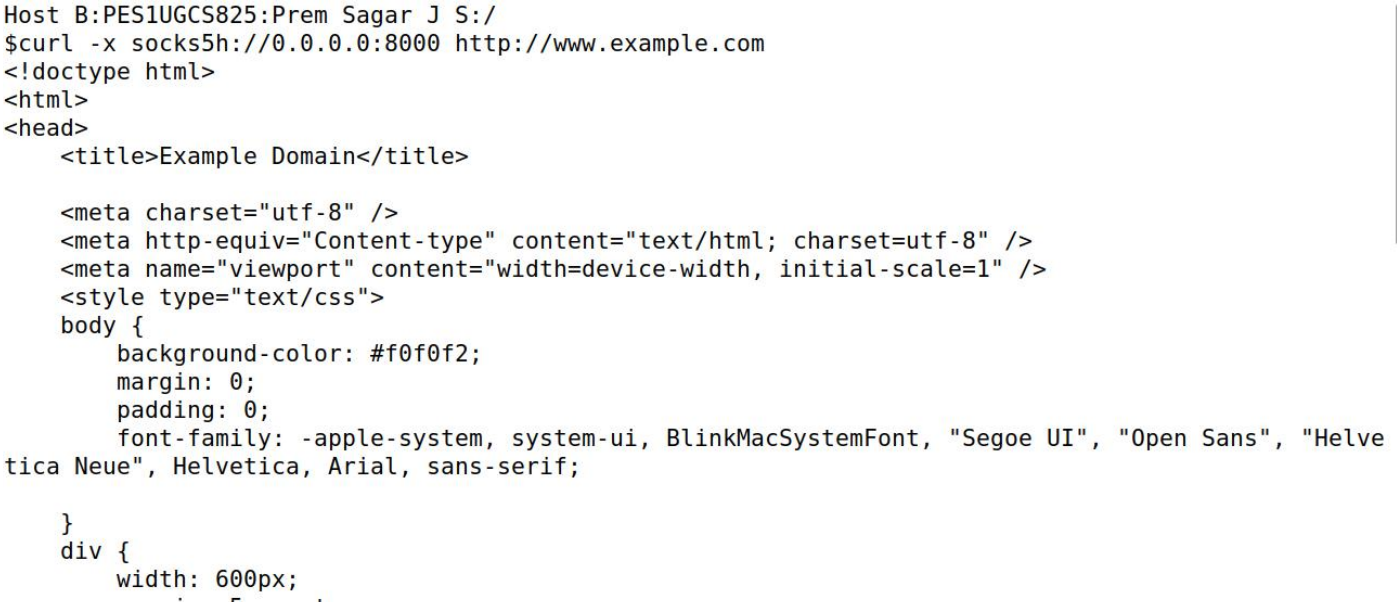
Machine on the external network with IP 10.8.0.99 will make the actual connection with the intended web server.

(2) How does this computer know which server it should connect to?

As this is a dynamic port forwading, we don’t mention the destination while adding the rule for the ssh tunneling so, the server address will be given by the machine which is initiating the request.

Run in container B:

```
# curl -x socks5h://0.0.0.0:8000 http://www.example.com
```

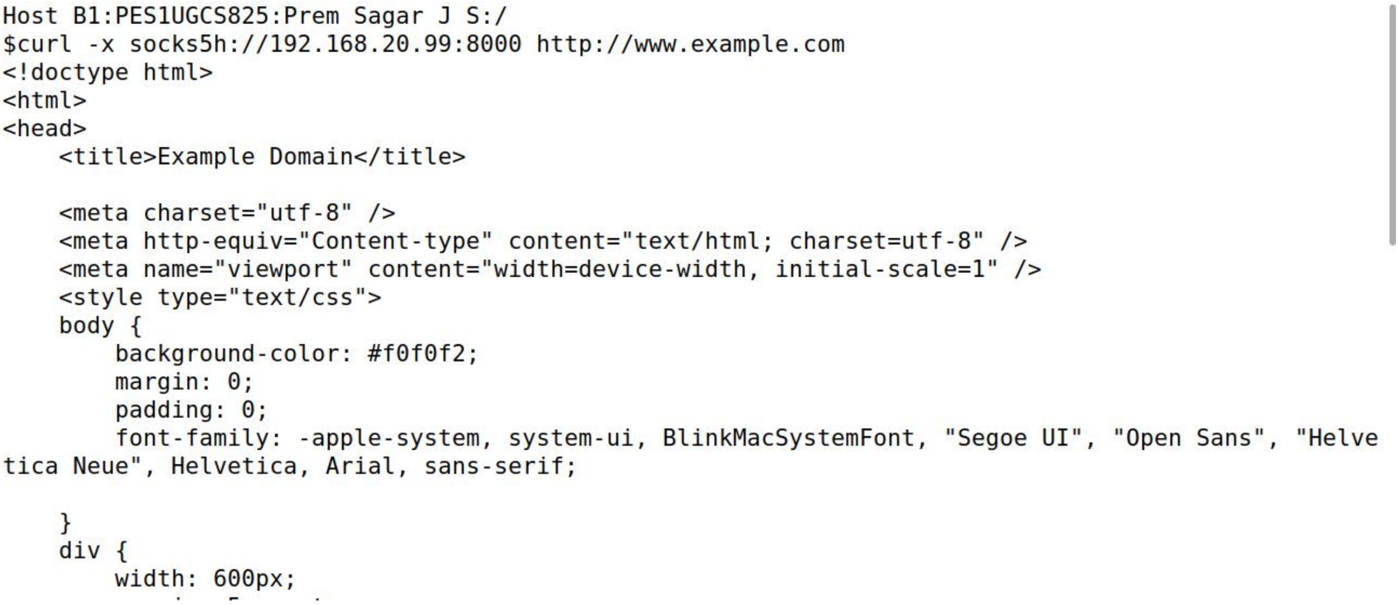


```
Host B:PES1UGCS825:Prem Sagar J S:/
$curl -x socks5h://0.0.0.0:8000 http://www.example.com
<!doctype html>
<html>
<head>
    <title>Example Domain</title>

    <meta charset="utf-8" />
    <meta http-equiv="Content-type" content="text/html; charset=utf-8" />
    <meta name="viewport" content="width=device-width, initial-scale=1" />
    <style type="text/css">
    body {
        background-color: #f0f0f2;
        margin: 0;
        padding: 0;
        font-family: -apple-system, system-ui, BlinkMacSystemFont, "Segoe UI", "Open Sans", "Helve
tica Neue", Helvetica, Arial, sans-serif;

    }
    div {
        width: 600px;
```

To access the websites from B1,B2 run the following command in the corresponding containers:

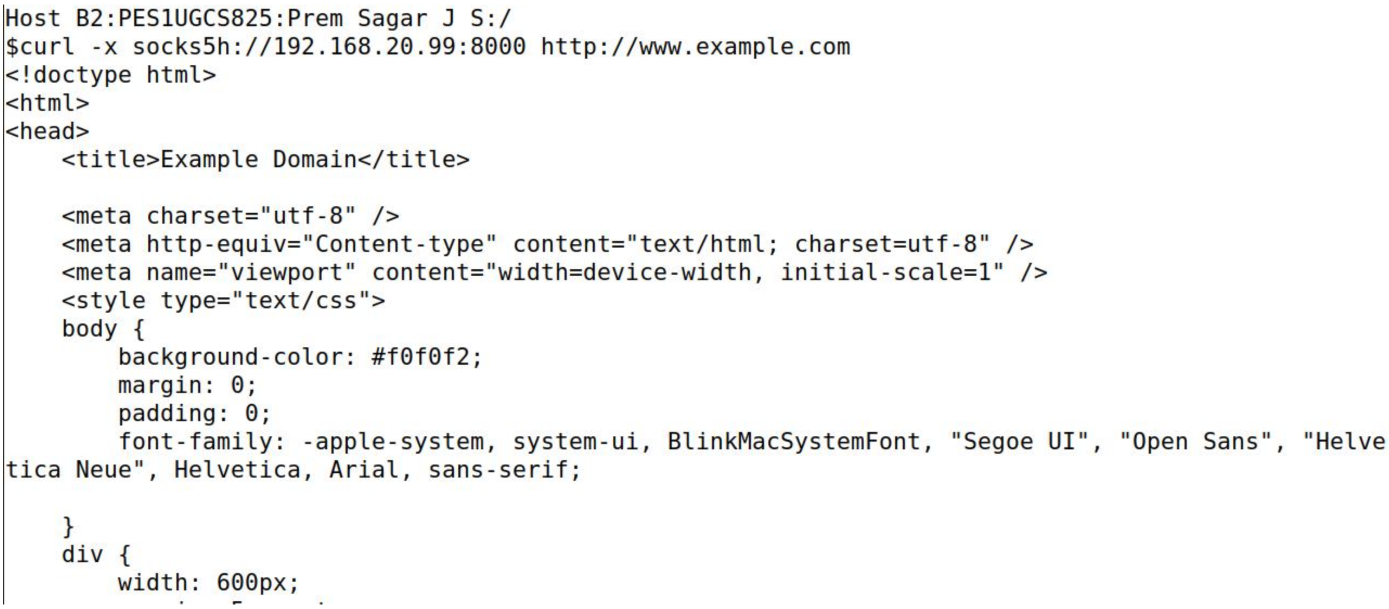
```
# curl -x socks5h://192.168.20.99:8000 http://www.example.com
```

On Host B1 :



```
Host B1:PES1UGCS825:Prem Sagar J S:/
$curl -x socks5h://192.168.20.99:8000 http://www.example.com
<!doctype html>
<html>
<head>
    <title>Example Domain</title>

    <meta charset="utf-8" />
    <meta http-equiv="Content-type" content="text/html; charset=utf-8" />
    <meta name="viewport" content="width=device-width, initial-scale=1" />
    <style type="text/css">
    body {
        background-color: #f0f0f2;
        margin: 0;
        padding: 0;
        font-family: -apple-system, system-ui, BlinkMacSystemFont, "Segoe UI", "Open Sans", "Helve
tica Neue", Helvetica, Arial, sans-serif;

    }
    div {
        width: 600px;
```

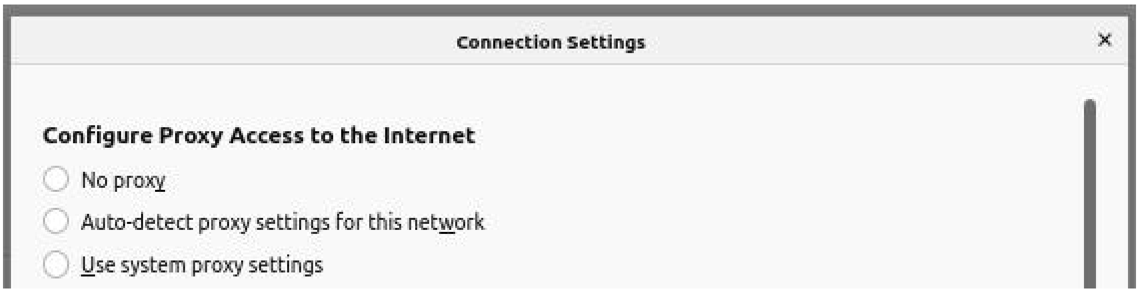
On Host B2 :



```
Host B2:PES1UGCS825:Prem Sagar J S:/
$curl -x socks5h://192.168.20.99:8000 http://www.example.com
<!doctype html>
<html>
<head>
    <title>Example Domain</title>

    <meta charset="utf-8" />
    <meta http-equiv="Content-type" content="text/html; charset=utf-8" />
    <meta name="viewport" content="width=device-width, initial-scale=1" />
    <style type="text/css">
    body {
        background-color: #f0f0f2;
        margin: 0;
        padding: 0;
        font-family: -apple-system, system-ui, BlinkMacSystemFont, "Segoe UI", "Open Sans", "Helve
tica Neue", Helvetica, Arial, sans-serif;

    }
    div {
        width: 600px;
```

## Task 2.2: Testing the Tunnel Using Browser

configuring Firefox's proxy setting.



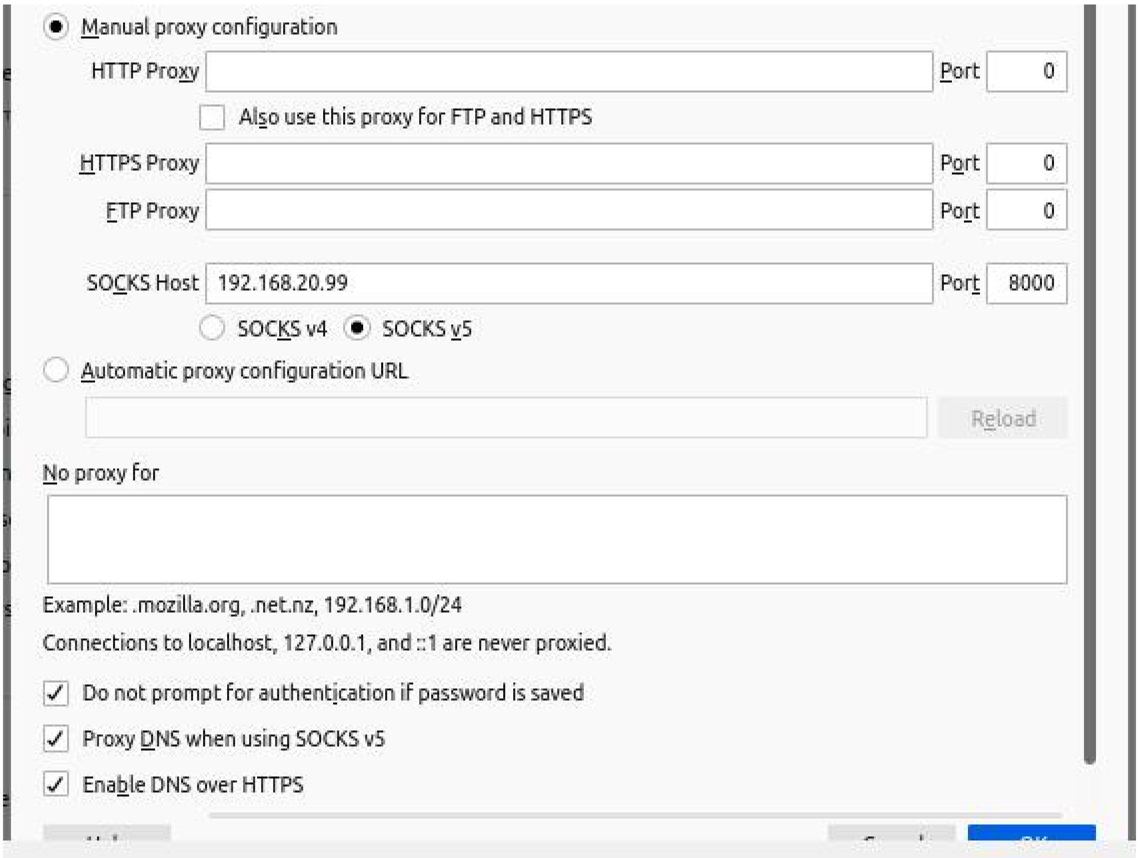
Connection Settings

Configure Proxy Access to the Internet

○ No proxy

○ Auto-detect proxy settings for this network

○ Use system proxy settings



● Manual proxy configuration

HTTP Proxy | Port 0

□ Also use this proxy for FTP and HTTPS

HTTPS Proxy | Port 0

FTP Proxy | Port 0

SOCKS Host 192.168.20.99 | Port 8000

○ SOCKS v4 ● SOCKS v5

○ Automatic proxy configuration URL

No proxy for

Example: .mozilla.org, .net.nz, 192.168.1.0/24

Connections to localhost, 127.0.0.1, and ::1 are never proxied.

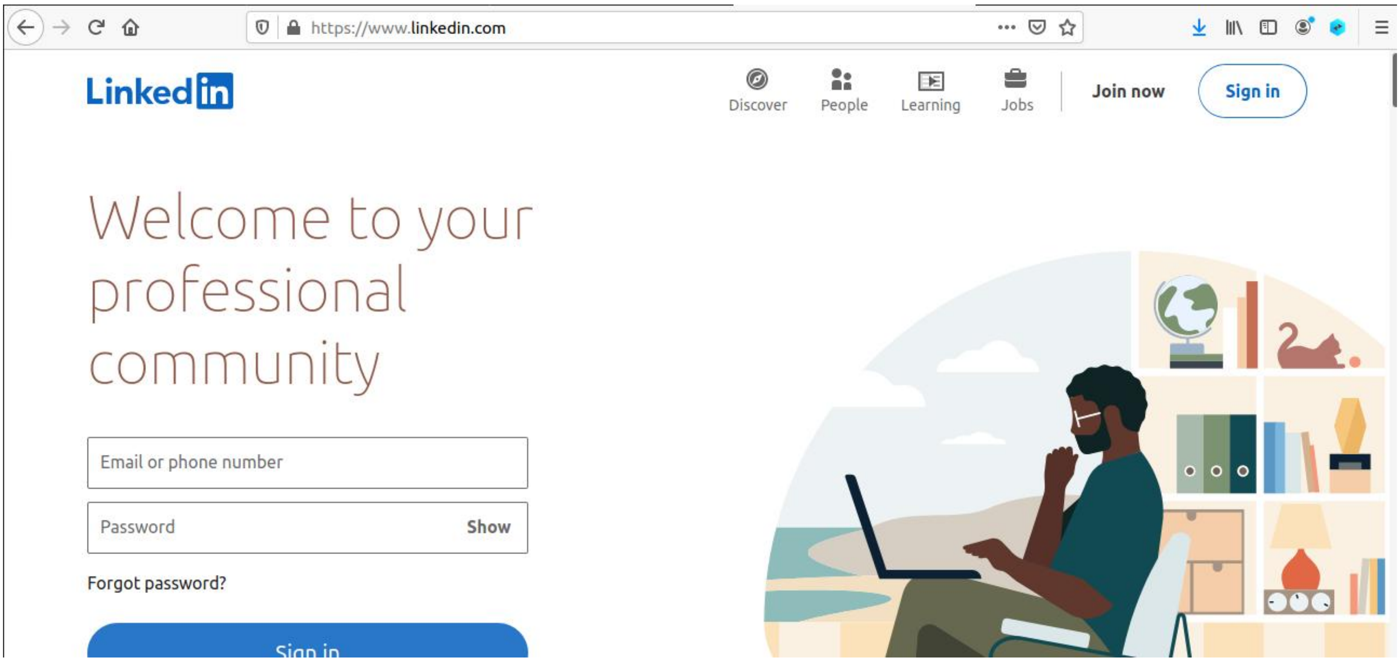
☑ Do not prompt for authentication if password is saved

☑ Proxy DNS when using SOCKS v5

☑ Enable DNS over HTTPS

Lab task. Once the proxy is configured, we can then browse any website. The requests and replies will go through the SSH tunnel. Since the host VM can reach the Internet directly, to make sure that our web browsing traffic has gone through the tunnel,

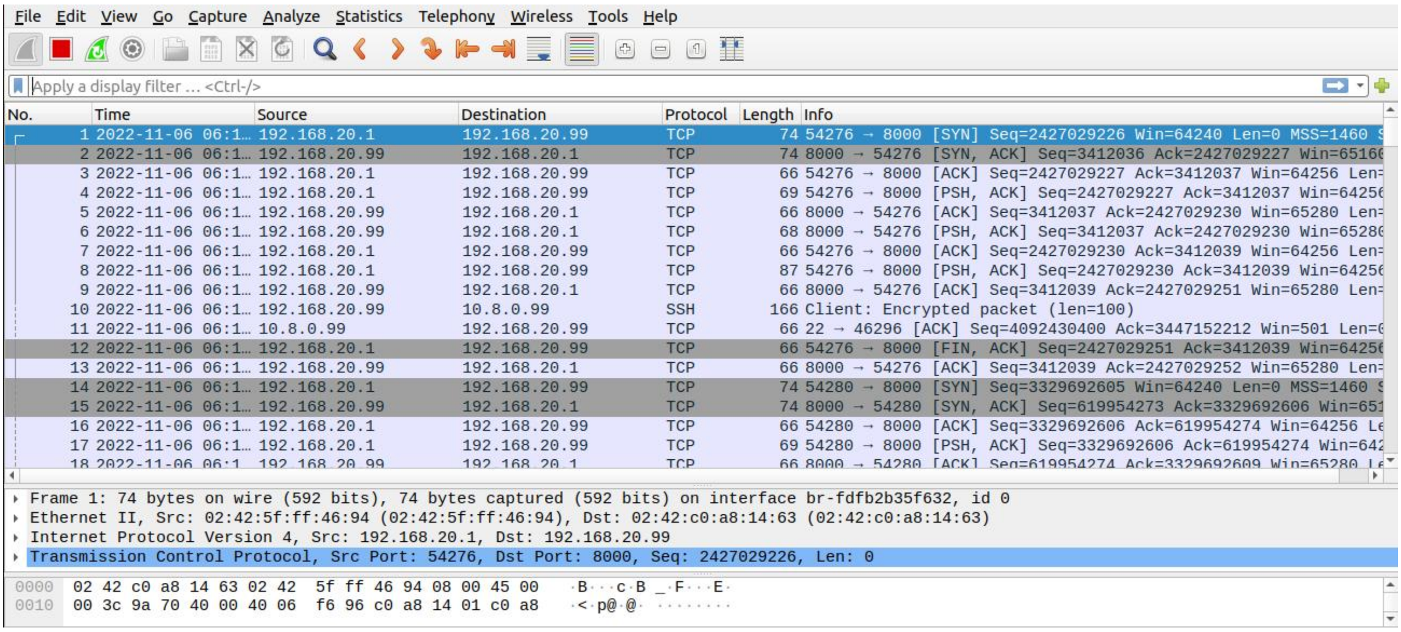
Trying to access the website after configuration :



https://www.linkedin.com

Welcome to your professional community

Wireshark Observation :



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.  Time                Source          Destination     Protocol Length Info
   1 2022-11-06 06:1… 192.168.20.1    192.168.20.99   TCP        74 54276 → 8000 [SYN] Seq=2427029226 Win=64240 Len=0 MSS=1460 S
   2 2022-11-06 06:1… 192.168.20.99   192.168.20.1    TCP        74 8000 → 54276 [SYN, ACK] Seq=3412036 Ack=2427029227 Win=65160
   3 2022-11-06 06:1… 192.168.20.1    192.168.20.99   TCP        66 54276 → 8000 [ACK] Seq=2427029227 Ack=3412037 Win=64256 Len=
   4 2022-11-06 06:1… 192.168.20.1    192.168.20.99   TCP        69 54276 → 8000 [PSH, ACK] Seq=2427029227 Ack=3412037 Win=64256
   5 2022-11-06 06:1… 192.168.20.99   192.168.20.1    TCP        66 8000 → 54276 [ACK] Seq=3412037 Ack=2427029230 Win=65280 Len=
   6 2022-11-06 06:1… 192.168.20.99   192.168.20.1    TCP        68 8000 → 54276 [PSH, ACK] Seq=3412037 Ack=2427029230 Win=65280
   7 2022-11-06 06:1… 192.168.20.1    192.168.20.99   TCP        66 54276 → 8000 [ACK] Seq=2427029230 Ack=3412039 Win=64256 Len=
   8 2022-11-06 06:1… 192.168.20.1    192.168.20.99   TCP        87 54276 → 8000 [PSH, ACK] Seq=2427029230 Ack=3412039 Win=64256
   9 2022-11-06 06:1… 192.168.20.99   192.168.20.1    TCP        66 8000 → 54276 [ACK] Seq=3412039 Ack=2427029251 Win=65280 Len=
  10 2022-11-06 06:1… 192.168.20.99   10.8.0.99       SSH       166 Client: Encrypted packet (len=100)
  11 2022-11-06 06:1… 10.8.0.99       192.168.20.99   TCP        66 22 → 46296 [ACK] Seq=4092430400 Ack=3447152212 Win=501 Len=0
  12 2022-11-06 06:1… 192.168.20.1    192.168.20.99   TCP        66 54276 → 8000 [FIN, ACK] Seq=2427029251 Ack=3412039 Win=64256
  13 2022-11-06 06:1… 192.168.20.99   192.168.20.1    TCP        66 8000 → 54276 [ACK] Seq=3412039 Ack=2427029252 Win=65280 Len=
  14 2022-11-06 06:1… 192.168.20.1    192.168.20.99   TCP        74 54280 → 8000 [SYN] Seq=3329692605 Win=64240 Len=0 MSS=1460 S
  15 2022-11-06 06:1… 192.168.20.99   192.168.20.1    TCP        74 8000 → 54280 [SYN, ACK] Seq=619954273 Ack=3329692606 Win=651
  16 2022-11-06 06:1… 192.168.20.1    192.168.20.99   TCP        66 54280 → 8000 [ACK] Seq=3329692606 Ack=619954274 Win=64256 Le
  17 2022-11-06 06:1… 192.168.20.1    192.168.20.99   TCP        69 54280 → 8000 [PSH, ACK] Seq=3329692606 Ack=619954274 Win=642
  18 2022-11-06 06:1… 192.168.20.99   192.168.20.1    TCP        66 8000 → 54280 [ACK] Seq=619954274 Ack=3329692609 Win=65280 Le

▸ Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface br-fdfb2b35f632, id 0
▸ Ethernet II, Src: 02:42:5f:ff:46:94 (02:42:5f:ff:46:94), Dst: 02:42:c0:a8:14:63 (02:42:c0:a8:14:63)
▸ Internet Protocol Version 4, Src: 192.168.20.1, Dst: 192.168.20.99
▸ Transmission Control Protocol, Src Port: 54276, Dst Port: 8000, Seq: 2427029226, Len: 0

0000  02 42 c0 a8 14 63 02 42  5f ff 46 94 08 00 45 00   ·B···c·B _·F···E·
0010  00 3c 9a 70 40 00 40 06  f6 96 c0 a8 14 01 c0 a8   ·<·p@·@· ········
```

To close the ssh shell that is in the background created using the previous "ssh -4 -D 0.0.0.0:8000 root@10.8.0.99 -f -N" command :

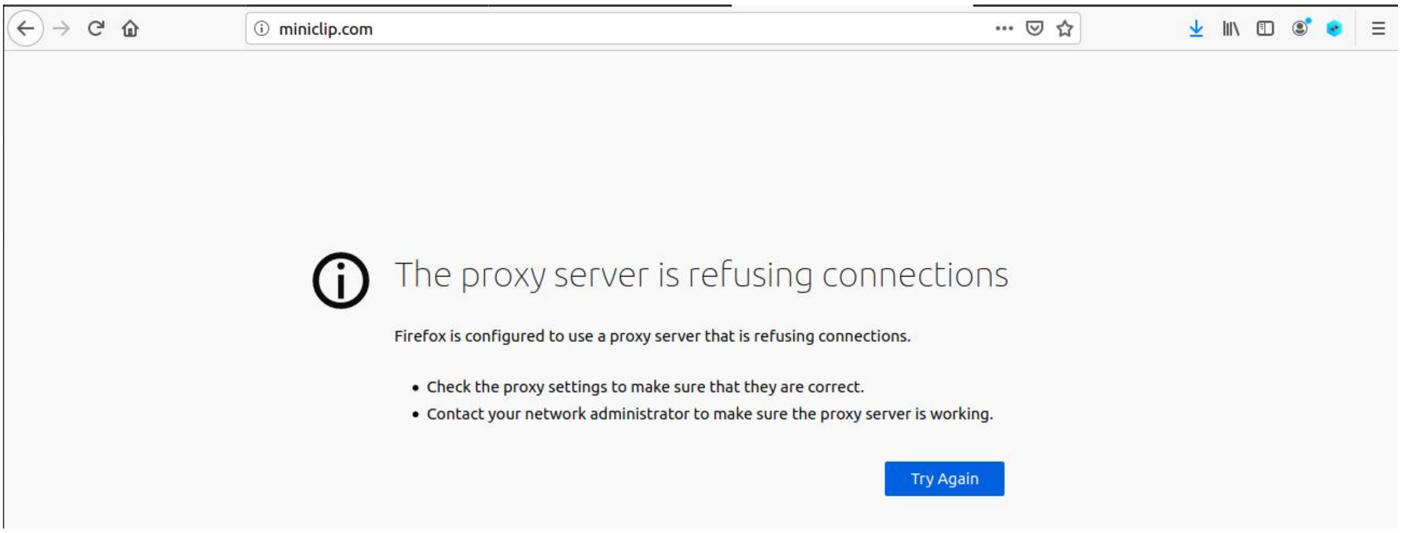
**Run the below commands in container B:**

**# ps -eaf | grep "ssh"**

**# kill [corresponding pid of the process]**

```
Host B:PES1UGCS825:Prem Sagar J S:/
$ps -eaf | grep "ssh"
root          38       1  0 10:09 ?        00:00:00 sshd: /usr/sbin/sshd [listener] 0 of 10-100 st
artups
root         147       1  0 10:43 ?        00:00:00 ssh -4 -D 0.0.0.0:8000 root@10.8.0.99 -f -N
root         149       1  0 10:43 ?        00:00:00 ssh -4 -D 0.0.0.0:8000 root@10.8.0.99 -f -N
root         157      40  0 11:14 pts/1    00:00:00 grep ssh
Host B:PES1UGCS825:Prem Sagar J S:/
$kill 147
Host B:PES1UGCS825:Prem Sagar J S:/
$kill 149
Host B:PES1UGCS825:Prem Sagar J S:/
$
```

Trying to connect the www.miniclip.com after the removing the SSH forwading :



The proxy server is refusing connections

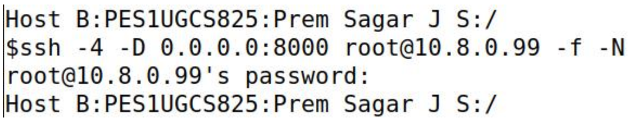
Firefox is configured to use a proxy server that is refusing connections.

- Check the proxy settings to make sure that they are correct.
- Contact your network administrator to make sure the proxy server is working.

Task 2.3: Writing a SOCKS Client Using Python

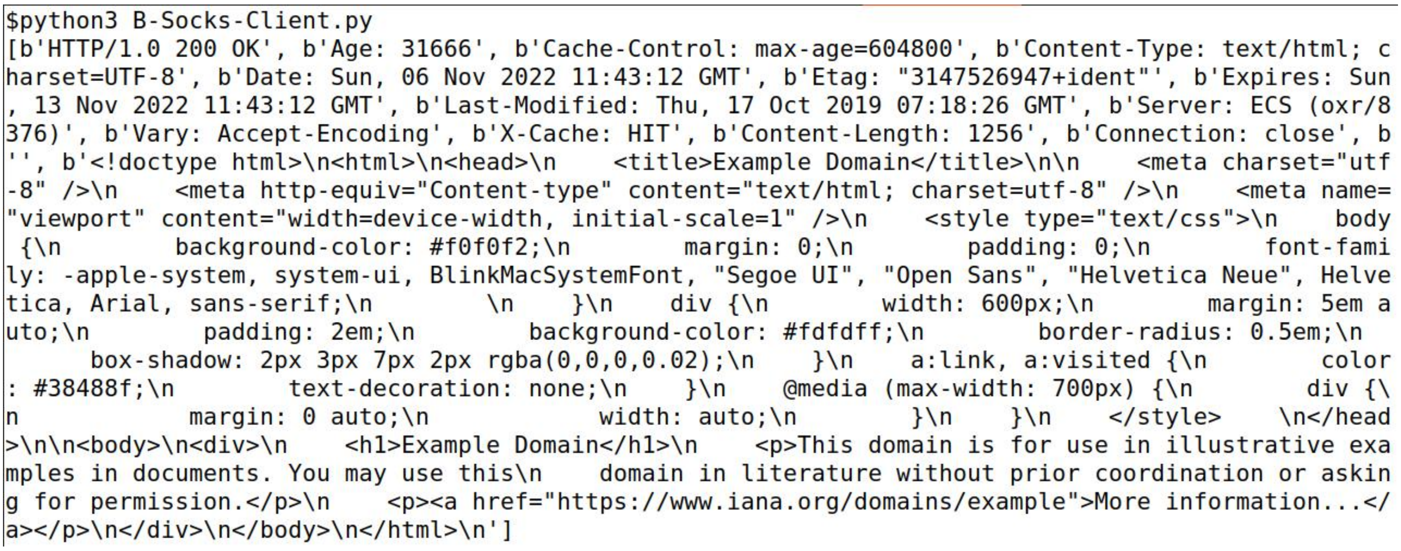
Lab task. Please complete this program, and use it to access http://www.example.com from hosts
B, B1, and B2. The code given above is only for sending HTTP requests, not HTTPS requests (sending HTTPS requests are much more complicated due to the TLS handshake). For this task, students only need to send HTTP requests.

Run in container B:
# ssh -4 -D 0.0.0.0:8000 root@10.8.0.99 -f -N



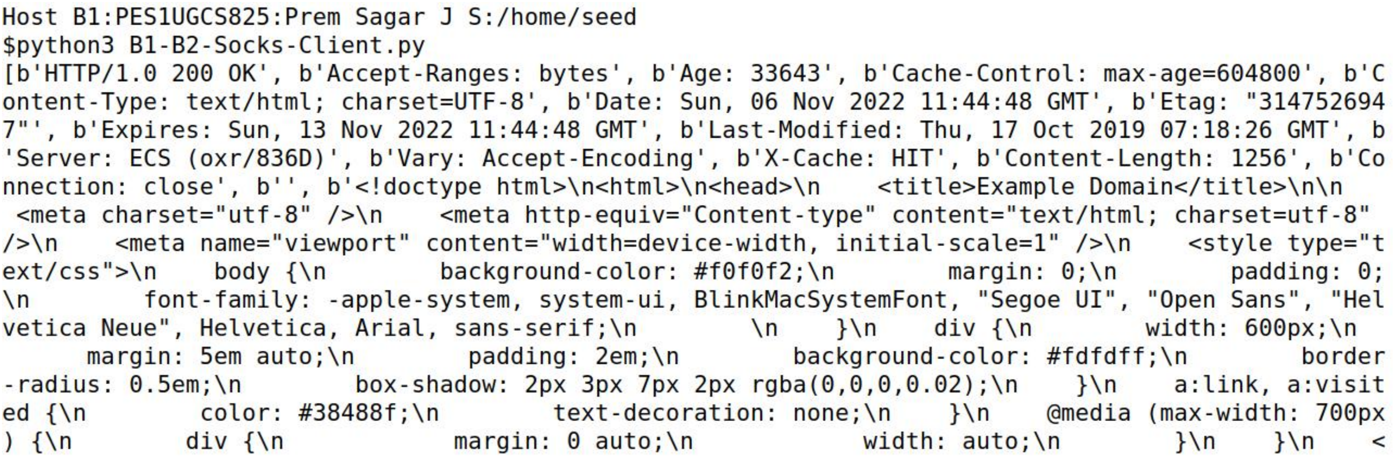
```
Host B:PES1UGCS825:Prem Sagar J S:/
$ssh -4 -D 0.0.0.0:8000 root@10.8.0.99 -f -N
root@10.8.0.99's password:
Host B:PES1UGCS825:Prem Sagar J S:/
```

Run in container B :
# python3 B-Socks-Client.py

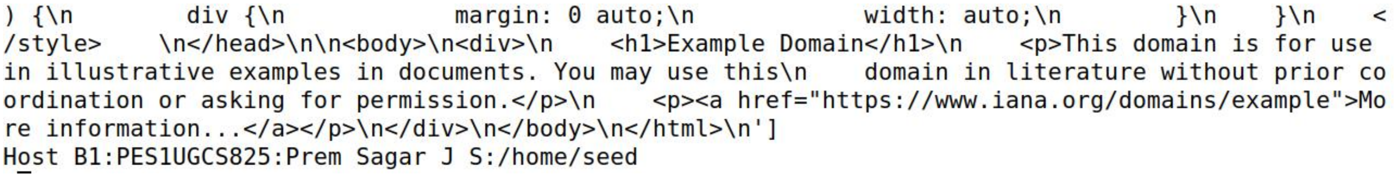


```
$python3 B-Socks-Client.py
[b'HTTP/1.0 200 OK', b'Age: 31666', b'Cache-Control: max-age=604800', b'Content-Type: text/html; c
harset=UTF-8', b'Date: Sun, 06 Nov 2022 11:43:12 GMT', b'Etag: "3147526947+ident"', b'Expires: Sun
, 13 Nov 2022 11:43:12 GMT', b'Last-Modified: Thu, 17 Oct 2019 07:18:26 GMT', b'Server: ECS (oxr/8
376)', b'Vary: Accept-Encoding', b'X-Cache: HIT', b'Content-Length: 1256', b'Connection: close', b
'', b'<!doctype html>\n<html>\n<head>\n    <title>Example Domain</title>\n\n    <meta charset="utf
-8" />\n    <meta http-equiv="Content-type" content="text/html; charset=utf-8" />\n    <meta name=
"viewport" content="width=device-width, initial-scale=1" />\n    <style type="text/css">\n    body
 {\n        background-color: #f0f0f2;\n        margin: 0;\n        padding: 0;\n        font-fami
ly: -apple-system, system-ui, BlinkMacSystemFont, "Segoe UI", "Open Sans", "Helvetica Neue", Helve
tica, Arial, sans-serif;\n        \n    }\n    div {\n        width: 600px;\n        margin: 5em a
uto;\n        padding: 2em;\n        background-color: #fdfdff;\n        border-radius: 0.5em;\n
      box-shadow: 2px 3px 7px 2px rgba(0,0,0,0.02);\n    }\n    a:link, a:visited {\n        color
: #38488f;\n        text-decoration: none;\n    }\n    @media (max-width: 700px) {\n        div {\
n            margin: 0 auto;\n            width: auto;\n        }\n    }\n    </style>    \n</head
>\n\n<body>\n<div>\n    <h1>Example Domain</h1>\n    <p>This domain is for use in illustrative exa
mples in documents. You may use this\n    domain in literature without prior coordination or askin
g for permission.</p>\n    <p><a href="https://www.iana.org/domains/example">More information...</
a></p>\n</div>\n</body>\n</html>\n']
```

Run in containers B1 and B2:
# python3 B1-B2-Socks-Client.py
On Container B1:

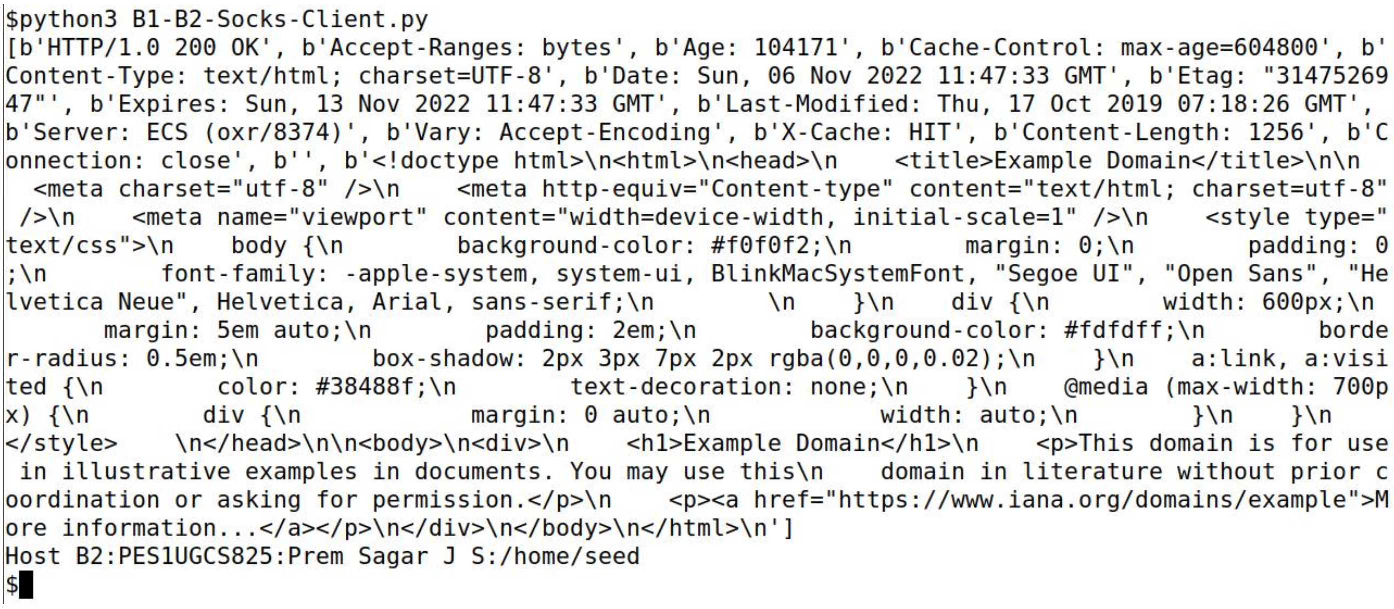


```
Host B1:PES1UGCS825:Prem Sagar J S:/home/seed
$python3 B1-B2-Socks-Client.py
[b'HTTP/1.0 200 OK', b'Accept-Ranges: bytes', b'Age: 33643', b'Cache-Control: max-age=604800', b'C
ontent-Type: text/html; charset=UTF-8', b'Date: Sun, 06 Nov 2022 11:44:48 GMT', b'Etag: "314752694
7"', b'Expires: Sun, 13 Nov 2022 11:44:48 GMT', b'Last-Modified: Thu, 17 Oct 2019 07:18:26 GMT', b
'Server: ECS (oxr/836D)', b'Vary: Accept-Encoding', b'X-Cache: HIT', b'Content-Length: 1256', b'Co
nnection: close', b'', b'<!doctype html>\n<html>\n<head>\n    <title>Example Domain</title>\n\n
 <meta charset="utf-8" />\n    <meta http-equiv="Content-type" content="text/html; charset=utf-8"
/>\n    <meta name="viewport" content="width=device-width, initial-scale=1" />\n    <style type="t
ext/css">\n    body {\n        background-color: #f0f0f2;\n        margin: 0;\n        padding: 0;
\n        font-family: -apple-system, system-ui, BlinkMacSystemFont, "Segoe UI", "Open Sans", "Hel
vetica Neue", Helvetica, Arial, sans-serif;\n        \n    }\n    div {\n        width: 600px;\n
      margin: 5em auto;\n        padding: 2em;\n        background-color: #fdfdff;\n        border
-radius: 0.5em;\n        box-shadow: 2px 3px 7px 2px rgba(0,0,0,0.02);\n    }\n    a:link, a:visit
ed {\n        color: #38488f;\n        text-decoration: none;\n    }\n    @media (max-width: 700px
) {\n        div {\n            margin: 0 auto;\n            width: auto;\n        }\n    }\n    <
```



```
) {\n        div {\n            margin: 0 auto;\n            width: auto;\n        }\n    }\n    <
/style>    \n</head>\n\n<body>\n<div>\n    <h1>Example Domain</h1>\n    <p>This domain is for use
in illustrative examples in documents. You may use this\n    domain in literature without prior co
ordination or asking for permission.</p>\n    <p><a href="https://www.iana.org/domains/example">Mo
re information...</a></p>\n</div>\n</body>\n</html>\n']
Host B1:PES1UGCS825:Prem Sagar J S:/home/seed
```

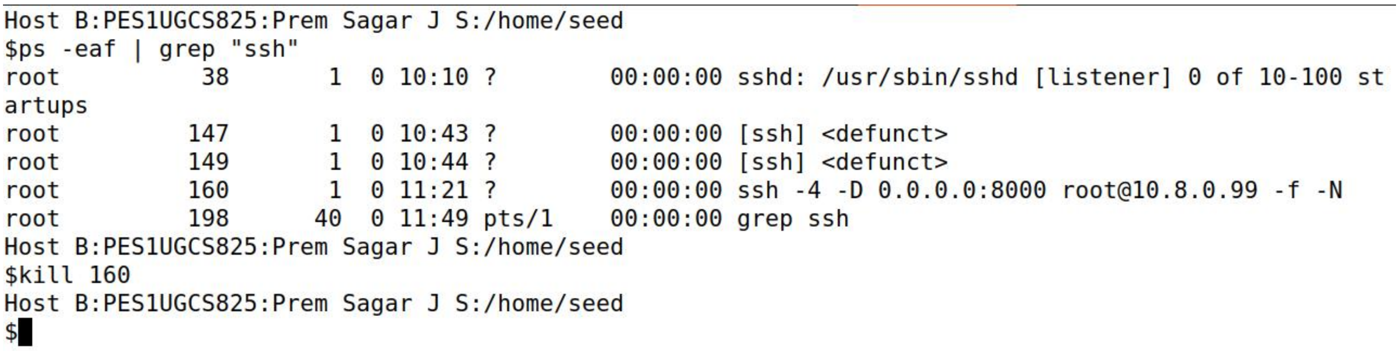
On Container B2:



```
$python3 B1-B2-Socks-Client.py
[b'HTTP/1.0 200 OK', b'Accept-Ranges: bytes', b'Age: 104171', b'Cache-Control: max-age=604800', b'
Content-Type: text/html; charset=UTF-8', b'Date: Sun, 06 Nov 2022 11:47:33 GMT', b'Etag: "31475269
47"', b'Expires: Sun, 13 Nov 2022 11:47:33 GMT', b'Last-Modified: Thu, 17 Oct 2019 07:18:26 GMT',
b'Server: ECS (oxr/8374)', b'Vary: Accept-Encoding', b'X-Cache: HIT', b'Content-Length: 1256', b'C
onnection: close', b'', b'<!doctype html>\n<html>\n<head>\n    <title>Example Domain</title>\n\n
  <meta charset="utf-8" />\n    <meta http-equiv="Content-type" content="text/html; charset=utf-8"
 />\n    <meta name="viewport" content="width=device-width, initial-scale=1" />\n    <style type="
text/css">\n    body {\n        background-color: #f0f0f2;\n        margin: 0;\n        padding: 0
;\n        font-family: -apple-system, system-ui, BlinkMacSystemFont, "Segoe UI", "Open Sans", "He
lvetica Neue", Helvetica, Arial, sans-serif;\n        \n    }\n    div {\n        width: 600px;\n
       margin: 5em auto;\n        padding: 2em;\n        background-color: #fdfdff;\n        borde
r-radius: 0.5em;\n        box-shadow: 2px 3px 7px 2px rgba(0,0,0,0.02);\n    }\n    a:link, a:visi
ted {\n        color: #38488f;\n        text-decoration: none;\n    }\n    @media (max-width: 700p
x) {\n        div {\n            margin: 0 auto;\n            width: auto;\n        }\n    }\n
</style>    \n</head>\n\n<body>\n<div>\n    <h1>Example Domain</h1>\n    <p>This domain is for use
 in illustrative examples in documents. You may use this\n    domain in literature without prior c
oordination or asking for permission.</p>\n    <p><a href="https://www.iana.org/domains/example">M
ore information...</a></p>\n</div>\n</body>\n</html>\n']
Host B2:PES1UGCS825:Prem Sagar J S:/home/seed
$
```

To close the ssh shell that is in the background created using the previous "ssh -4 -D 0.0.0.0:8000 root@10.8.0.99 -f -N" command :

```
# ps -eaf | grep "ssh"
# kill [corresponding pid of the process]
```



```
Host B:PES1UGCS825:Prem Sagar J S:/home/seed
$ps -eaf | grep "ssh"
root          38       1  0 10:10 ?        00:00:00 sshd: /usr/sbin/sshd [listener] 0 of 10-100 st
artups
root         147       1  0 10:43 ?        00:00:00 [ssh] <defunct>
root         149       1  0 10:44 ?        00:00:00 [ssh] <defunct>
root         160       1  0 11:21 ?        00:00:00 ssh -4 -D 0.0.0.0:8000 root@10.8.0.99 -f -N
root         198      40  0 11:49 pts/1    00:00:00 grep ssh
Host B:PES1UGCS825:Prem Sagar J S:/home/seed
$kill 160
Host B:PES1UGCS825:Prem Sagar J S:/home/seed
$
```

## Task 3: Comparing SOCKS5 Proxy and VPN

An HTTP proxy works similarly to SOCKS5 when it comes to creating outbound TCP connections and gaining access to servers beyond the firewall.

However, the most significant difference is that the HTTP proxy carefully inspects and filters the network traffic to only process requests made by the HTTP protocol.

The SOCKS5 proxy is better for acquiring raw, unfiltered data that you wish to process manually. Meanwhile, the HTTP protocol is a faster solution for leaving out any irrelevant data outside of HTTP, great for users who want to save a lot of time.

It can identify duplicate requests to reply from the cache, thus boosting performance by eliminating unnecessary resource-consuming operations. HTTP is more intelligent but less secure than SOCKS5.

## Advantages of using SOCKS5

- Hides your IP address and doesn’t hamper your connection speed because it doesn’t encrypt the network traffic.
- Unlocks websites which are otherwise unavailable to you due to geographical restrictions or censorship.
- Excellent for establishing TCP connections outside the firewall.
- Excellent speed for downloading or uploading torrents.
- Excellent solution when more bandwidth is required (if you are using a limited data plan, for example).
- Some torrent trackers halt operations if SOCKS5 is not enabled.
- More secure than other proxy servers.
- Works with both TCP and UDP connections.
- There are tons of websites offering free SOCK5 proxy lists, like Socks-Proxy, Proxy-List, SocksList and ProxyRack.
- Easy to configure and doesn’t need you to install additional applications. You can manually set up SOCKS5 within your web browser, add a free proxy browser extension, or quickly install apply a proxy configuration to your torrent client.

## Disadvantages of using SOCKS5

- Cannot encrypt your network traffic.
- Cannot protect you from hackers when connecting to public hotspots. They might sniff your network to find login data and credit card info.
- Cannot hide your browsing activity from your ISP or prevent bandwidth throttling.
- Cannot preserve your anonymity when downloading or uploading torrents with copyright material.
- Not efficient for unlocking streaming content on sites such as Netflix, which quickly identifies and blocks proxy servers.
- Some torrent trackers block SOCKS5 proxies.

## Advantages of using VPN

- Can hide your IP address and encrypt your network traffic, too.

- Prevents your ISP from snooping around to see what websites you’ re visiting.
- Protects you from hackers when traveling and connecting to public Wi-Fi, like airports, hotels, coffee shops, and rest areas.
- Keeps you safe from government surveillance, particularly if you’ re living in a 5, 9, 14 Eyes country.
- Helps you get around Netflix blocks to unlock movies and TV shows that are not available to your country.
- Offers servers from many countries to connect.

## Disadvantages of using VPN

- Slower Internet connections, especially when using a faulty configuration.
- Excellent service is not cheap. You would have to pay a monthly or yearly subscription to benefit from round-the-clock VPN features.
- Free VPNs can cause disastrous effects on uninformed users since these services might collect and sell your data to marketing companies, or turn you into an endpoint to improve the bandwidth of premium users.