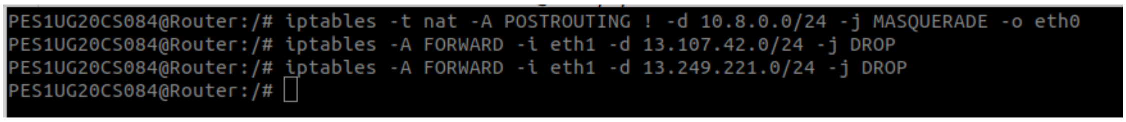
CNS Lab 8 Firewall Evasion

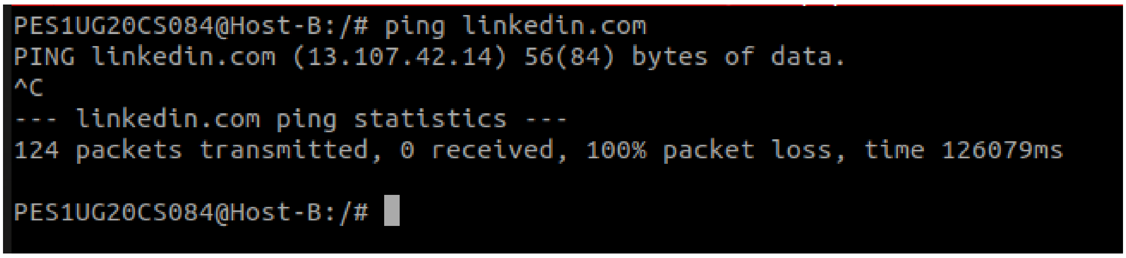
PES1UG20CS084

Aryansh Bhargavan

Task 0: Get Familiar with the Lab Setup



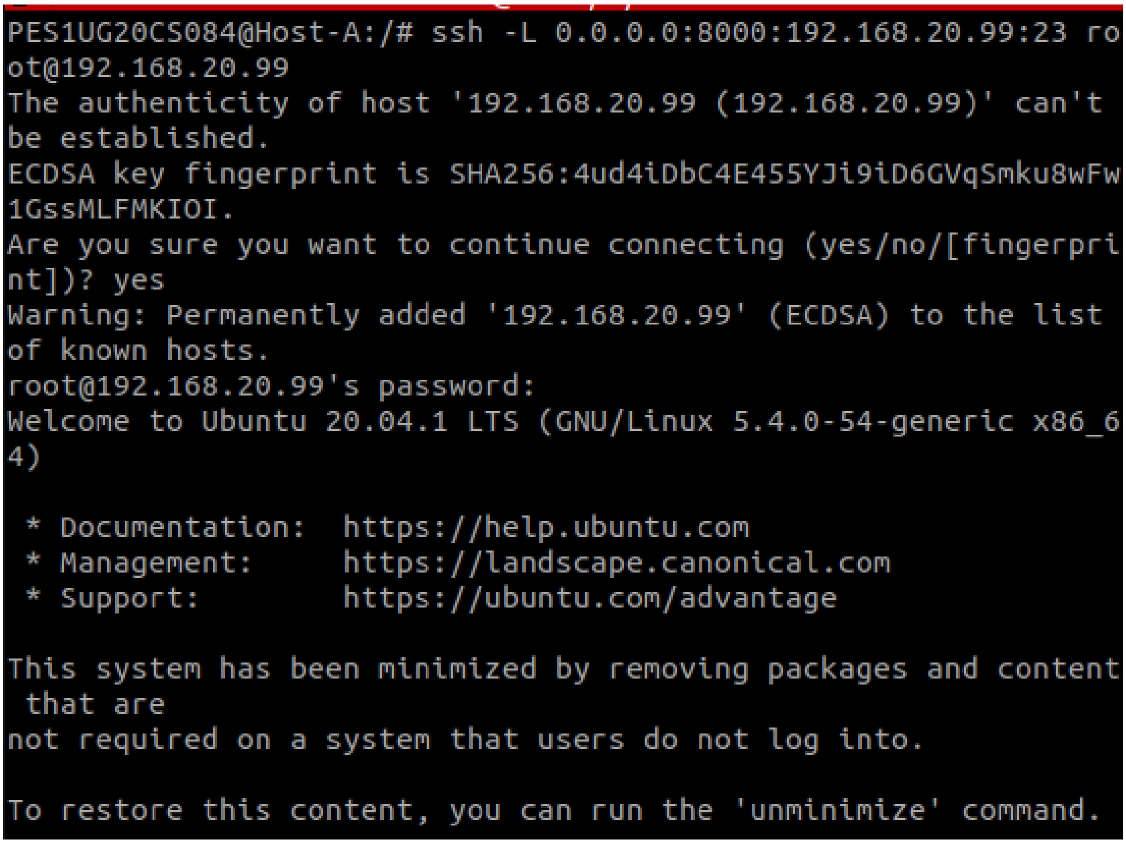
```
PES1UG20CS084@Router:/# iptables -t nat -A POSTROUTING ! -d 10.8.0.0/24 -j MASQUERADE -o eth0
PES1UG20CS084@Router:/# iptables -A FORWARD -i eth1 -d 13.107.42.0/24 -j DROP
PES1UG20CS084@Router:/# iptables -A FORWARD -i eth1 -d 13.249.221.0/24 -j DROP
PES1UG20CS084@Router:/# 
```



```
PES1UG20CS084@Host-B:/# ping linkedin.com
PING linkedin.com (13.107.42.14) 56(84) bytes of data.
^C
--- linkedin.com ping statistics ---
124 packets transmitted, 0 received, 100% packet loss, time 126079ms

PES1UG20CS084@Host-B:/# 
```

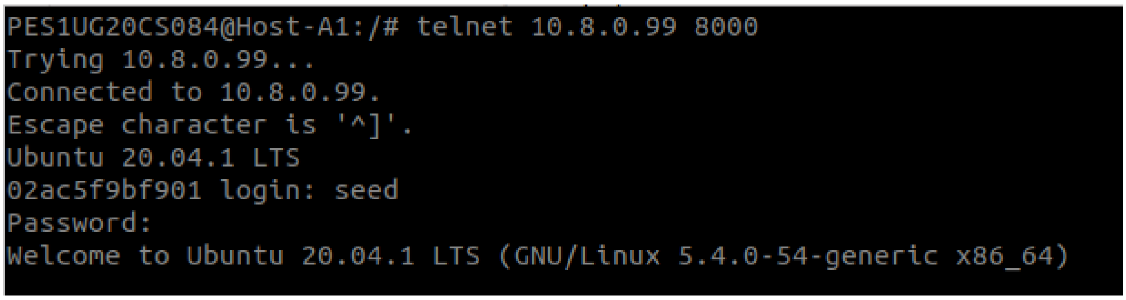
Task 1 : Static Port Forwarding

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

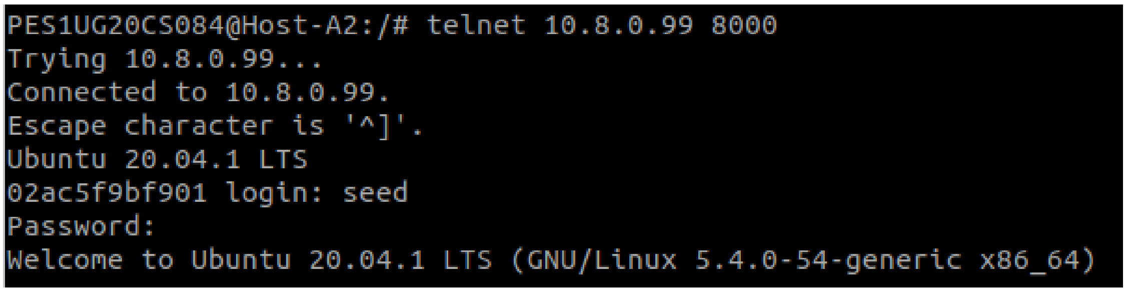


```
PES1UG20CS084@Host-A:/# ssh -L 0.0.0.0:8000:192.168.20.99:23 ro
ot@192.168.20.99
The authenticity of host '192.168.20.99 (192.168.20.99)' can't
be established.
ECDSA key fingerprint is SHA256:4ud4iDbC4E455YJi9iD6GVqSmku8wFw
1GssMLFMKIOI.
Are you sure you want to continue connecting (yes/no/[fingerpri
nt])? yes
Warning: Permanently added '192.168.20.99' (ECDSA) to the list
of known hosts.
root@192.168.20.99's password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_6
4)

 * 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.
```

```
# telnet 10.8.0.99 8000
```



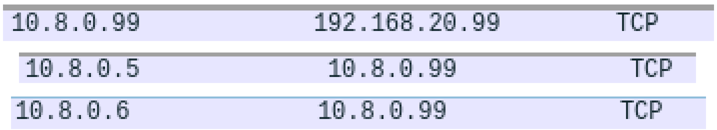
```
PES1UG20CS084@Host-A1:/# telnet 10.8.0.99 8000
Trying 10.8.0.99...
Connected to 10.8.0.99.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
02ac5f9bf901 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)
```



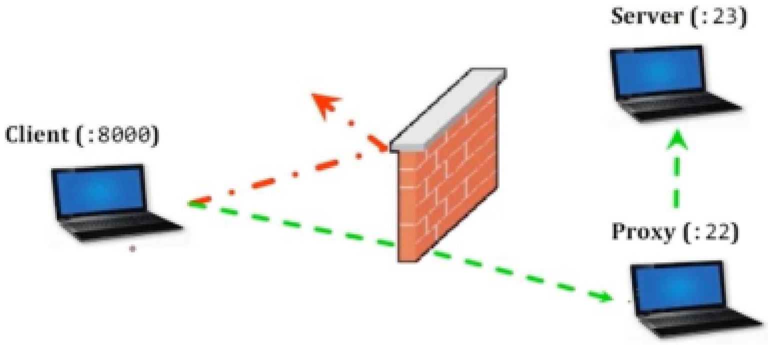
```
PES1UG20CS084@Host-A2:/# telnet 10.8.0.99 8000
Trying 10.8.0.99...
Connected to 10.8.0.99.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
02ac5f9bf901 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)
```

Questions

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

> 
>
> | | | |
> |---|---|---|
> | 10.8.0.99 | 192.168.20.99 | TCP |
> | 10.8.0.5 | 10.8.0.99 | TCP |
> | 10.8.0.6 | 10.8.0.99 | TCP |
>
> There are 3 TCP connections, between A and router, A1 - A, and A2 - A.

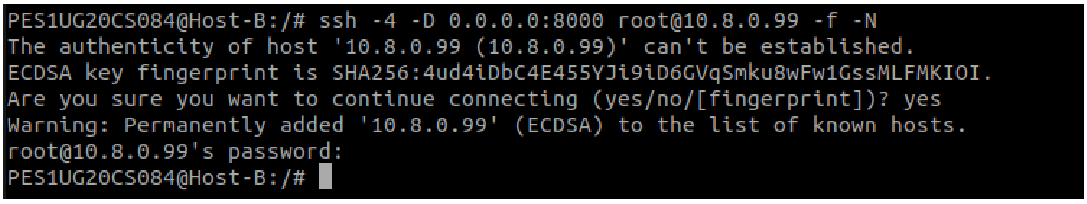
2. Why can this tunnel successfully help users evade the firewall rule specified in the lab setup?

> This can be explained with this diagram
>
> 
>
>
> Since client does not have access to a service, they use an ssh tunnel for data forwarding. As recorded traffic is only between client and the proxy, it evades the firewall. (This is valid only if SSH is also not restricted by firewall as in the case of PESU)

Task 2: Dynamic Port Forwarding

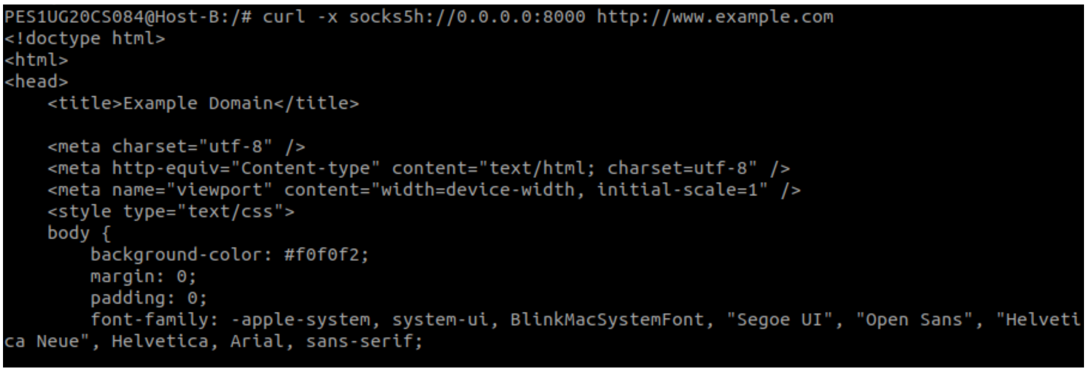
Task 2.1: Setting Up Dynamic Port Forwarding

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



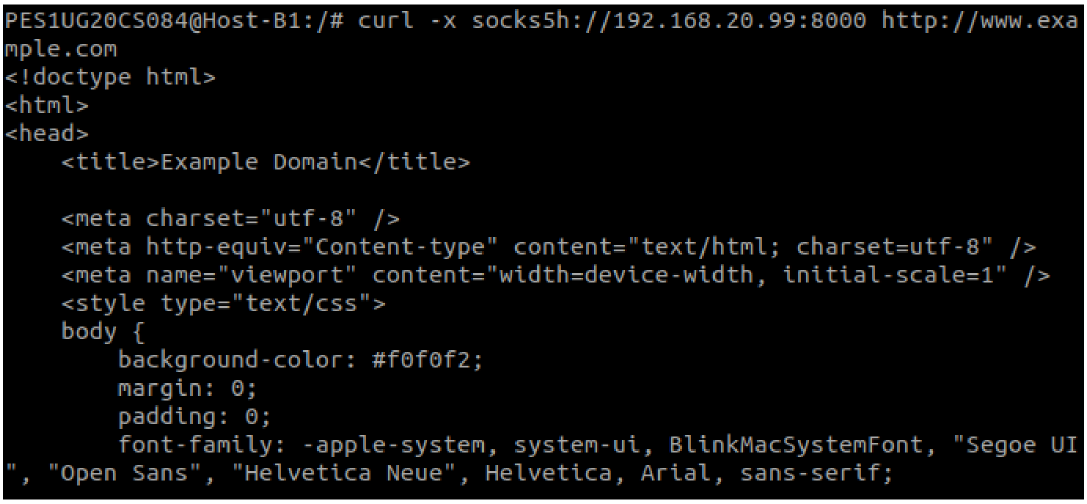
```
PES1UG20CS084@Host-B:/# ssh -4 -D 0.0.0.0:8000 root@10.8.0.99 -f -N
The authenticity of host '10.8.0.99 (10.8.0.99)' can't be established.
ECDSA key fingerprint is SHA256:4ud4iDbC4E455YJi9iD6GVqSmku8wFw1GssMLFMKIOI.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.8.0.99' (ECDSA) to the list of known hosts.
root@10.8.0.99's password:
PES1UG20CS084@Host-B:/# 
```

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

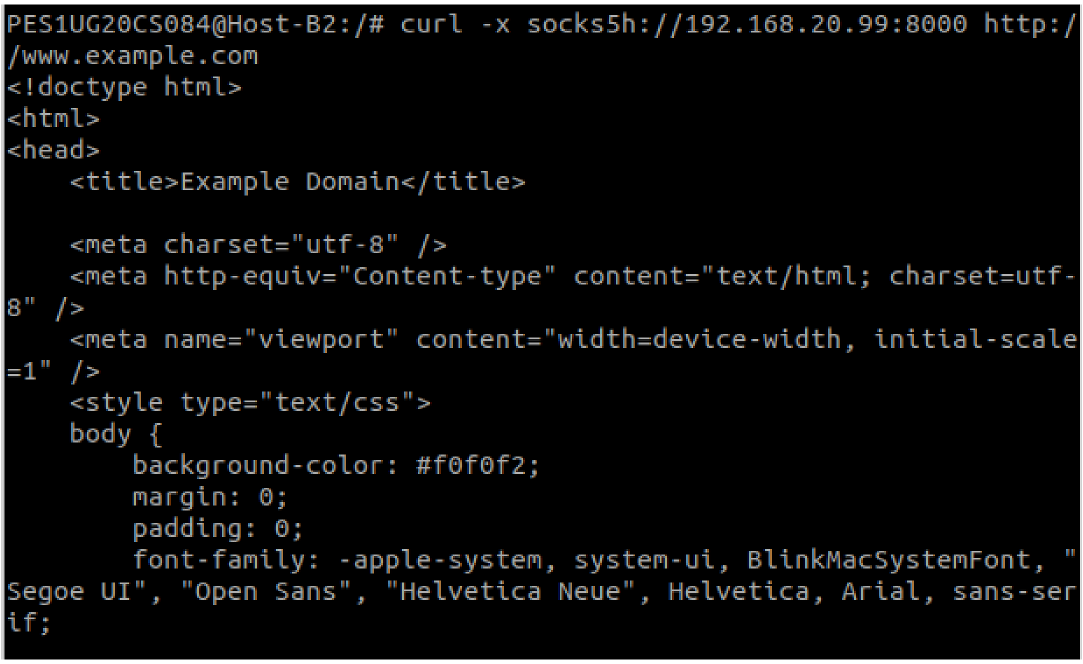


```
PES1UG20CS084@Host-B:/# curl -x socks5h://0.0.0.0:8000 http://www.example.com
<!doctype html>
<html>
<head>
    <title>Example Domain</title>

    <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", "Helveti
ca Neue", Helvetica, Arial, sans-serif;
```

Trying to access blocked website from B1 and B2



```
PES1UG20CS084@Host-B1:/# curl -x socks5h://192.168.20.99:8000 http://www.exa
mple.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", "Helvetica Neue", Helvetica, Arial, sans-serif;
```



```
PES1UG20CS084@Host-B2:/# 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", "Helvetica Neue", Helvetica, Arial, sans-ser
if;
```

Questions

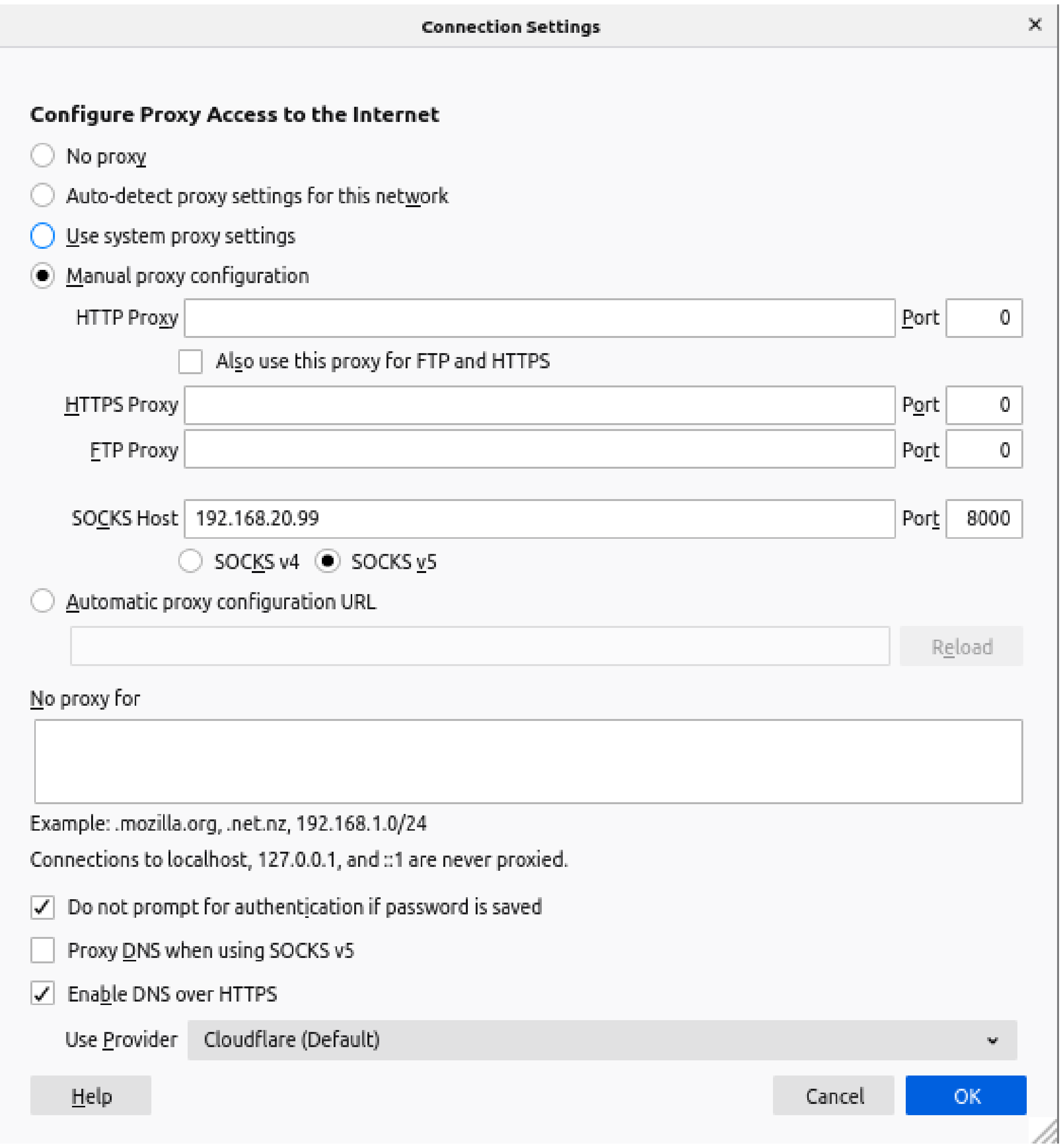
1. Which computer establishes the actual connection with the intended web server?

   > Host B acts as the proxy between client (host b1, b2) and hence establishes the actual connection with intended web server

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

   > Once the client asks the proxy to connect to a web server, this is first received by the proxy, and then forwarded on behalf of the proxy. The proxy receives request data and acts like a regular computer accessing said request data. The response data is then forwarded to the client, thus accessing data restricted by the firewall.

Task 2.2: Testing the Tunnel Using Browser



Configure Proxy Access to the Internet

○ No proxy

○ Auto-detect proxy settings for this network

○ Use system proxy settings

● Manual proxy configuration

HTTP Proxy: (empty) Port: 0

□ Also use this proxy for FTP and HTTPS

HTTPS Proxy: (empty) Port: 0

FTP Proxy: (empty) 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

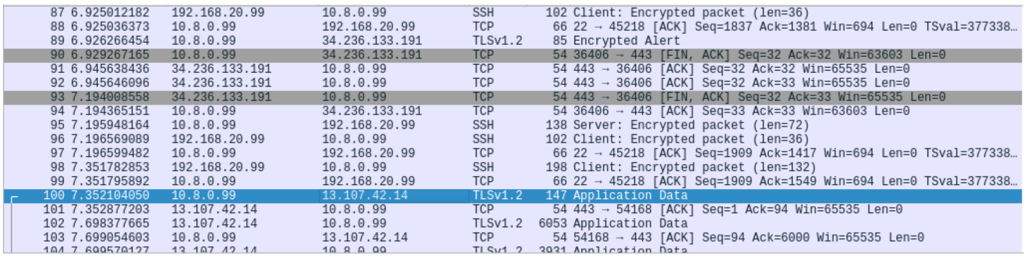
□ Proxy DNS when using SOCKS v5

☑ Enable DNS over HTTPS

Use Provider: Cloudflare (Default)

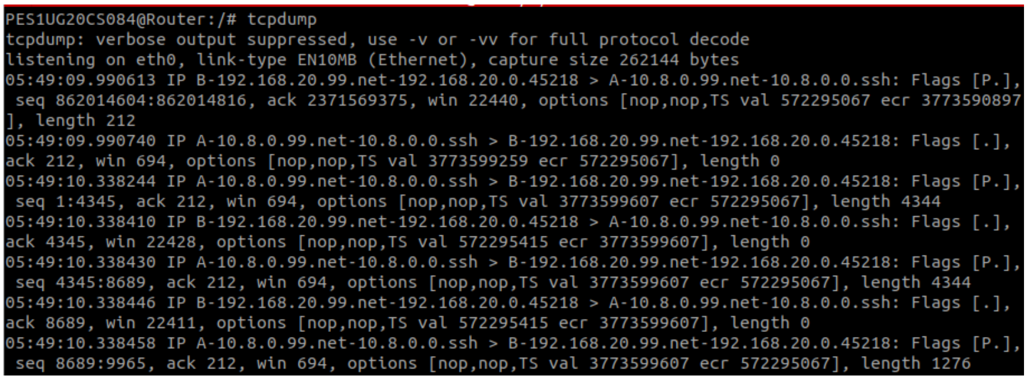
Questions

1. Run tcpdump on the router-firewall, and point out the traffic involved in the entire port forwarding process



```
 87 6.925012182  192.168.20.99  10.8.0.99      SSH      102 Client: Encrypted packet (len=36)
 88 6.925036373  10.8.0.99      192.168.20.99  TCP       66 22 → 45218 [ACK] Seq=1837 Ack=1381 Win=694 Len=0 TSval=377338…
 89 6.926266454  10.8.0.99      34.236.133.191 TLSv1.2   85 Encrypted Alert
 90 6.929267165  10.8.0.99      34.236.133.191 TCP       54 36406 → 443 [FIN, ACK] Seq=32 Ack=32 Win=63603 Len=0
 91 6.945638436  34.236.133.191 10.8.0.99      TCP       54 443 → 36406 [ACK] Seq=32 Ack=32 Win=65535 Len=0
 92 6.945646096  34.236.133.191 10.8.0.99      TCP       54 443 → 36406 [ACK] Seq=32 Ack=33 Win=65535 Len=0
 93 7.194008558  34.236.133.191 10.8.0.99      TCP       54 443 → 36406 [FIN, ACK] Seq=32 Ack=33 Win=65535 Len=0
 94 7.194365151  10.8.0.99      34.236.133.191 TCP       54 36406 → 443 [ACK] Seq=33 Ack=33 Win=63603 Len=0
 95 7.195948164  10.8.0.99      192.168.20.99  SSH      138 Server: Encrypted packet (len=72)
 96 7.196569089  192.168.20.99  10.8.0.99      SSH      102 Client: Encrypted packet (len=36)
 97 7.196599482  10.8.0.99      192.168.20.99  TCP       66 22 → 45218 [ACK] Seq=1909 Ack=1417 Win=694 Len=0 TSval=377338…
 98 7.351782853  192.168.20.99  10.8.0.99      SSH      198 Client: Encrypted packet (len=132)
 99 7.351795892  10.8.0.99      192.168.20.99  TCP       66 22 → 45218 [ACK] Seq=1909 Ack=1549 Win=694 Len=0 TSval=377338…
100 7.352104050  10.8.0.99      13.107.42.14   TLSv1.2  147 Application Data
101 7.352877203  13.107.42.14   10.8.0.99      TCP       54 443 → 54168 [ACK] Seq=1 Ack=94 Win=65535 Len=0
102 7.698377665  13.107.42.14   10.8.0.99      TLSv1.2 6053 Application Data
103 7.699054603  10.8.0.99      13.107.42.14   TCP       54 54168 → 443 [ACK] Seq=94 Ack=6000 Win=65535 Len=0
104 7.699570127  13.107.42.14   10.8.0.99      TLSv1.2 3931 Application Data
```

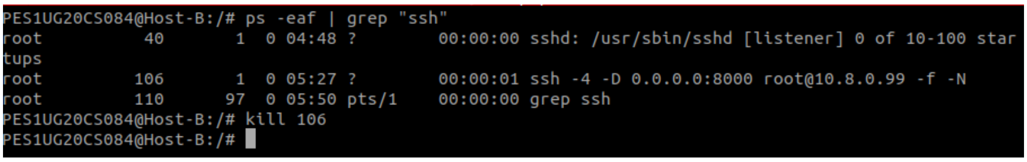
tcpdump on router



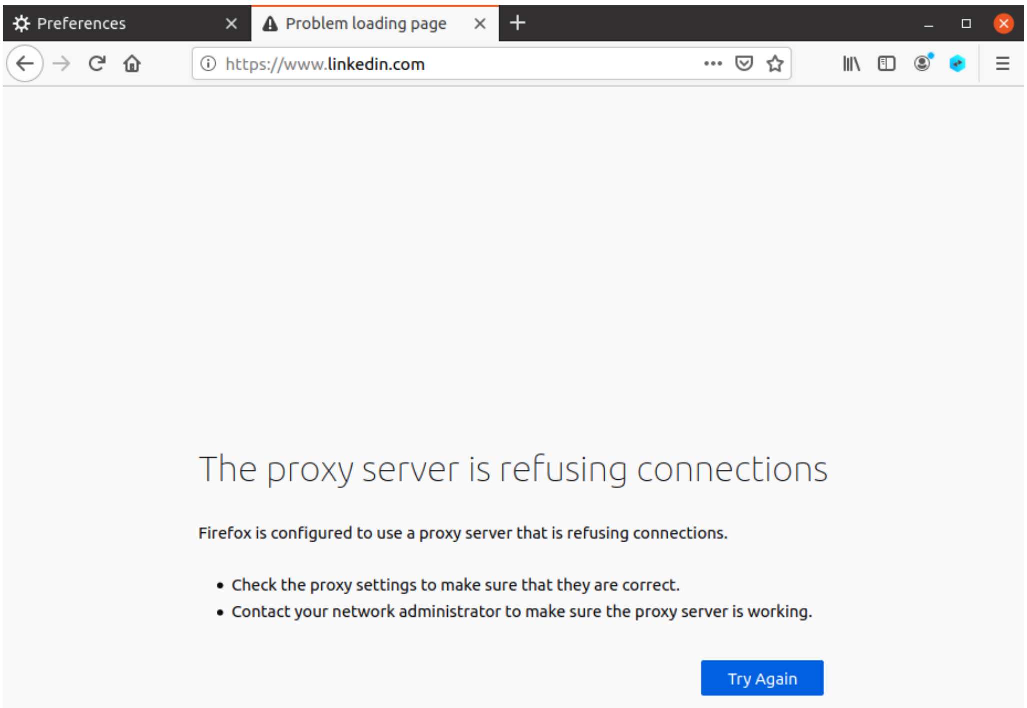
```
PES1UG20CS084@Router:/# tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
05:49:09.990613 IP B-192.168.20.99.net-192.168.20.0.45218 > A-10.8.0.99.net-10.8.0.0.ssh: Flags [P.],
 seq 862014604:862014816, ack 2371569375, win 22440, options [nop,nop,TS val 572295067 ecr 3773590897
], length 212
05:49:09.990740 IP A-10.8.0.99.net-10.8.0.0.ssh > B-192.168.20.99.net-192.168.20.0.45218: Flags [.],
ack 212, win 694, options [nop,nop,TS val 3773599259 ecr 572295067], length 0
05:49:10.338244 IP A-10.8.0.99.net-10.8.0.0.ssh > B-192.168.20.99.net-192.168.20.0.45218: Flags [P.],
 seq 1:4345, ack 212, win 694, options [nop,nop,TS val 3773599607 ecr 572295067], length 4344
05:49:10.338410 IP B-192.168.20.99.net-192.168.20.0.45218 > A-10.8.0.99.net-10.8.0.0.ssh: Flags [.],
ack 4345, win 22428, options [nop,nop,TS val 572295415 ecr 3773599607], length 0
05:49:10.338430 IP A-10.8.0.99.net-10.8.0.0.ssh > B-192.168.20.99.net-192.168.20.0.45218: Flags [P.],
 seq 4345:8689, ack 212, win 694, options [nop,nop,TS val 3773599607 ecr 572295067], length 4344
05:49:10.338446 IP B-192.168.20.99.net-192.168.20.0.45218 > A-10.8.0.99.net-10.8.0.0.ssh: Flags [.],
ack 8689, win 22411, options [nop,nop,TS val 572295415 ecr 3773599607], length 0
05:49:10.338458 IP A-10.8.0.99.net-10.8.0.0.ssh > B-192.168.20.99.net-192.168.20.0.45218: Flags [P.],
 seq 8689:9965, ack 212, win 694, options [nop,nop,TS val 3773599607 ecr 572295067], length 1276
```

We can see that the ssh tunnel is being used

2. Break the SSH tunnel, and then try to browse a website. Describe your observation



```
PES1UG20CS084@Host-B:/# ps -eaf | grep "ssh"
root          40       1  0 04:48 ?        00:00:00 sshd: /usr/sbin/sshd [listener] 0 of 10-100 star
tups
root         106       1  0 05:27 ?        00:00:01 ssh -4 -D 0.0.0.0:8000 root@10.8.0.99 -f -N
root         110      97  0 05:50 pts/1    00:00:00 grep ssh
PES1UG20CS084@Host-B:/# kill 106
PES1UG20CS084@Host-B:/# 
```



The proxy server is refusing connections

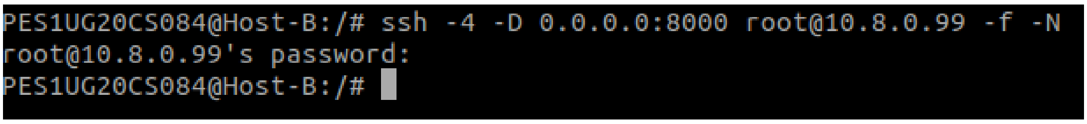
Firefox is configured to use a proxy server that is refusing connections.

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

Since ssh tunnel has been broken, we are no longer able to access `linkedin.com`

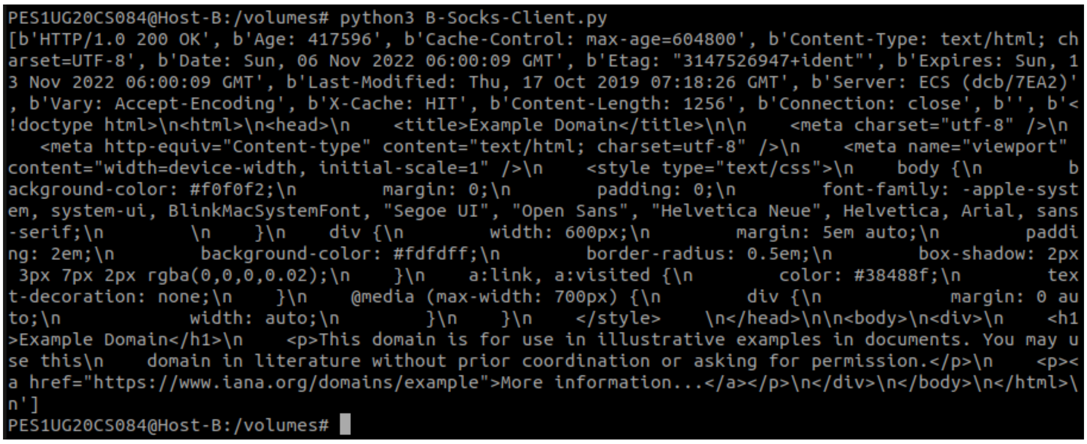
Task 2.3: Writing a SOCKS Client Using Python

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



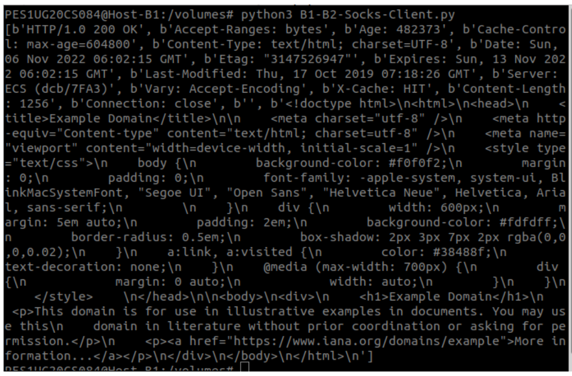
```
PES1UG20CS084@Host-B:/# ssh -4 -D 0.0.0.0:8000 root@10.8.0.99 -f -N
root@10.8.0.99's password:
PES1UG20CS084@Host-B:/# 
```

`# python3 B-Socks-Client.py`

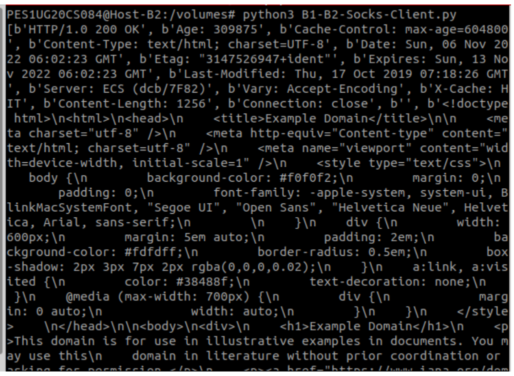


```
PES1UG20CS084@Host-B:/volumes# python3 B-Socks-Client.py
[b'HTTP/1.0 200 OK', b'Age: 417596', b'Cache-Control: max-age=604800', b'Content-Type: text/html; ch
arset=UTF-8', b'Date: Sun, 06 Nov 2022 06:00:09 GMT', b'Etag: "3147526947+ident"', b'Expires: Sun, 1
3 Nov 2022 06:00:09 GMT', b'Last-Modified: Thu, 17 Oct 2019 07:18:26 GMT', b'Server: ECS (dcb/7EA2)'
, 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        b
ackground-color: #f0f0f2;\n        margin: 0;\n        padding: 0;\n        font-family: -apple-syst
em, system-ui, BlinkMacSystemFont, "Segoe UI", "Open Sans", "Helvetica Neue", Helvetica, Arial, sans
-serif;\n        \n    }\n    div {\n        width: 600px;\n        margin: 5em auto;\n        paddi
ng: 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        tex
t-decoration: none;\n    }\n    @media (max-width: 700px) {\n        div {\n            margin: 0 au
to;\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 u
se this\n    domain in literature without prior coordination or asking for permission.</p>\n    <p><
a href="https://www.iana.org/domains/example">More information...</a></p>\n</div>\n</body>\n</html>\
n']
PES1UG20CS084@Host-B:/volumes# 
```

On Host b1 and b2



```
PES1UG20CS084@Host-B1:/volumes# python3 B1-B2-Socks-Client.py
[b'HTTP/1.0 200 OK', b'Accept-Ranges: bytes', b'Age: 482373', b'Cache-Contro
l: max-age=604800', b'Content-Type: text/html; charset=UTF-8', b'Date: Sun,
06 Nov 2022 06:02:15 GMT', b'Etag: "3147526947"', b'Expires: Sun, 13 Nov 202
2 06:02:15 GMT', b'Last-Modified: Thu, 17 Oct 2019 07:18:26 GMT', b'Server:
ECS (dcb/7FA3)', 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-family: -apple-system, system-ui, Bl
inkMacSystemFont, "Segoe UI", "Open Sans", "Helvetica Neue", Helvetica, Aria
l, sans-serif;\n        \n    }\n    div {\n        width: 600px;\n        m
argin: 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: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 examples in documents. You may us
e this\n    domain in literature without prior coordination or asking for pe
rmission.</p>\n    <p><a href="https://www.iana.org/domains/example">More in
formation...</a></p>\n</div>\n</body>\n</html>\n']
PES1UG20CS084@Host-B1:/volumes# 
```



```
PES1UG20CS084@Host-B2:/volumes# python3 B1-B2-Socks-Client.py
[b'HTTP/1.0 200 OK', b'Age: 309875', b'Cache-Control: max-age=604800
', b'Content-Type: text/html; charset=UTF-8', b'Date: Sun, 06 Nov 20
22 06:02:23 GMT', b'Etag: "3147526947+ident"', b'Expires: Sun, 13 No
v 2022 06:02:23 GMT', b'Last-Modified: Thu, 17 Oct 2019 07:18:26 GMT
', b'Server: ECS (dcb/7F82)', b'Vary: Accept-Encoding', b'X-Cache: H
IT', b'Content-Length: 1256', b'Connection: close', b'', b'<!doctype
 html>\n<html>\n<head>\n    <title>Example Domain</title>\n\n    <me
ta charset="utf-8" />\n    <meta http-equiv="Content-type" content="
text/html; charset=utf-8" />\n    <meta name="viewport" content="wid
th=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, B
linkMacSystemFont, "Segoe UI", "Open Sans", "Helvetica Neue", Helvet
ica, Arial, sans-serif;\n        \n    }\n    div {\n        width:
600px;\n        margin: 5em auto;\n        padding: 2em;\n        ba
ckground-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:vis
ited {\n        color: #38488f;\n        text-decoration: none;\n
 }\n    @media (max-width: 700px) {\n        div {\n            marg
in: 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 m
ay use this\n    domain in literature without prior coordination or
asking for permission.</p>\n    <p><a href="https://www.iana.org/dom
```

We can access said website since it is being forwarded using the ssh proxy

Task 3: Comparing SOCKS5 Proxy and VPN

SOCKS5

- Proxy server
- Faster that VPN (Lack of encryption)
- Uses SSH
- Easy and cheap to set up

VPN

- Also proxy server
- Encrypted traffic, so more secure
- Also makes it slower (due to encryption)
- Makes tunnel preventing IP address to access data that you are accessing
- Speed depends on VPN server location also
- Costly to set up