Suppose you lived & studied at a repressive institution that didn’t want to let its students communicate with the outside world. They have a firewall on the gateway into the institution’s network that drops incoming packets bound for any port other than port 22. They do this to stop students from, for instance, putting up their own webservers with pictures and stories about the injustices they face. (They allow port 22 so Profs can work at home.) Explain how you could run a webserver off your computer (which is inside the network) none-the-less, and explain what extra information (meaning in addition to your IP address) folks outside the network would need in order to access your underground website?

1. Consider Configuration A, B, and C pictured below:

Configuration A:

```
0.1.2.3.4 Firewall 0.5.6.7.8
```

Configuration B:

```
0.1.2.3.4 Router Firewall 0.5.6.7.8
```

Configuration C:

```
0.1.2.3.4 Router Router Firewall 0.5.6.7.8
```

If the firewall is configured to drop all packets with destination port 22, then ... 

i. Configuration ____ stops host 1.2.3.4 from connecting via SSH to any host. Explain!

ii. Configuration ____ stops any host from connecting to host 5.6.7.8 via SSH. Explain!
2. Suppose we have the following network configuration, in which the firewall drops all traffic with destination port equal to 80, and forwards everything else:

```
1.2.3.4  Router  Firewall  Router  5.6.7.8
|       |             |           |            |
1.2.3.5 |             |       |            |
```

a. Can host 5.6.7.8 access a DNS name server running on host 1.2.3.5? Explain!

b. Can host 5.6.7.8 access a web server running on host 5.6.7.9? Explain!

c. Can host 5.6.7.8 access a web server running on host 1.2.3.4? Explain!

d. Suppose host 5.6.7.8 has an SSH connection to host 1.2.3.5 running in its terminal window. If the command `nc 1.2.3.4 80` was typed into that terminal window, would the connection to 1.2.3.4 on port 80 be made, or would the firewall prevent it? Explain!

3. Consider these two versions of an ACL for a firewall:

**Version 1:**
- Drop packets from 22.10.133.8 going to TCP port 15000 on 87.52.8.125
- Forward packets from Any IP going to TCP port 15000 on 87.52.8.125

**Version 2:**
- Forward packets from Any IP going to TCP port 15000 on 87.52.8.125
- Drop packets from 22.10.133.8 going to TCP port 15000 on 87.52.8.125

(a) Which version allows all hosts other than 22.10.133.8 to connect via TCP to Host 87.52.8.125 on port 15000? (b) Explain why this is not true for the other version.