SI110 Introduction to Cyber Security AY12S
Technical Foundations

Name: _____

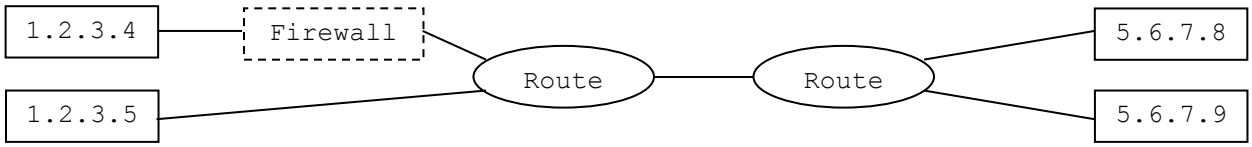
Alpha: _____

Hand in a stapled, printed copy with your answers.

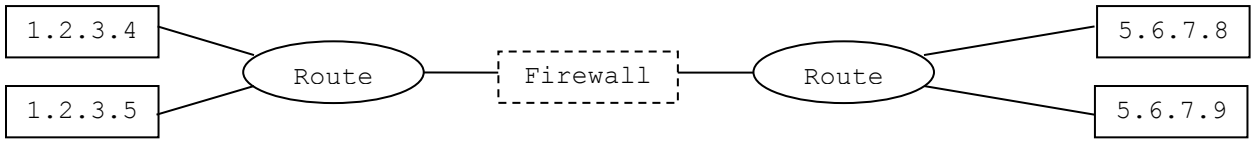
Homework: /SI110/Models and Tools/Firewalls

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

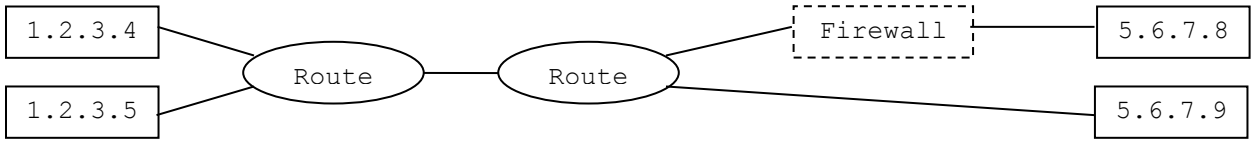
Configuration A:



Configuration B:



Configuration C:

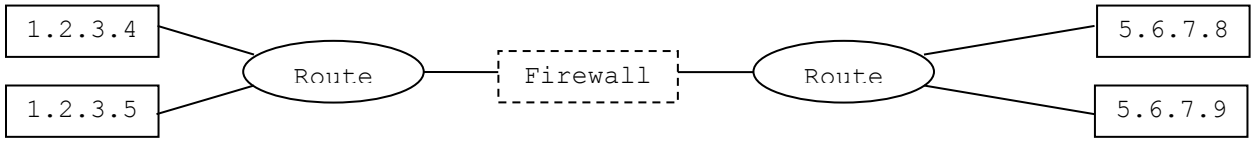


If the only firewall rule is to **drop all packets with destination port 22**, then…

i. Which configuration stops host 1.2.3.4 from connecting via SSH to any host. Explain.

ii. Which configuration stops any host from connecting to host 5.6.7.8 via SSH. Explain!

2. Suppose we have the following network configuration. The firewall drops all traffic with destination port 80, and forwards everything else:



Hand in a stapled, printed copy with your answers.

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 you are on 5.6.7.8 and you have a terminal/SSH connection to host 1.2.3.5. Host 1.2.3.4 is running a web server. If the command *nc 1.2.3.4 80* was typed into your terminal window, would the connection 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	12.50.13.8	going to	TCP port	15000	on	77.52.8.125
Forward	packets from	Any IP	going to	TCP port	15000	on	77.52.8.125

Version 2:

Forward	packets from	Any IP	going to	TCP port	15000	on	77.32.80.15
Drop	packets from	12.50.13.8	going to	TCP port	15000	on	77.32.80.15

Which of the two versions allows all hosts, except 12.50.13.8, to connect via TCP to Host 77.32.80.15 on port 15000? Explain!