Network Security

BSCH4

Assignment 1

This assignment is GRADED and will count toward your continuous assessment.

Time: you have two weeks from date of issue to complete

This is an individual assignment. Any work that is not your own that you do not correctly attribute will be considered pagiarism and will result in a score of ZERO being awarded for the entire assignment.

_____

Question 1. (30 marks)

Given the layout depicted in the network diagram shown in figure 1 below, write a set of firewall rules so that:

LAN: 192.168.0.0\24

Guest VLAN: 10.10.0.0\24

DMZ: 192.168.1.0\24

Clients on the internal LAN (192.168.0.0\24) have access to both the Intranet server and the web portal as well as the Internet in general.

Systems on the Guest VLAN (10.10.0.0\24) do not have access to the Intranet but can access the Internet and the web portal.

External users have access to the Web portal but not the intranet/extranet/LAN or guest VLAN

Systems on the Guest VLAN cannot directly interact with systems on the LAN

Intranet/Extranet server at 192.168.1.99 runs Antivirus software that listens for requests on port 2500 , an internal company web services server on port 80 and an email server on port 25. The user on system 192.168.0.12 is the server administrator and needs SSH access to the Intranet server on port 22.

The Web Portal hosts the customer website and web applications. Customer connect using HTTPS: and signed certificates (port 443). Only the Customer Services Support Technician at 192.168.0.20 should have access to the web portal server on port 22 (SSH) for updates and troubleshooting.

Assumptions:

All IP addresses are static

The firewalls are basic layer 3 firewalls (basic rule-based matching only but "state" is remembered)

All rules are directional with **IN** meaning traffic coming **FROM** the external network and **OUT** being traffic **TO** the external network.

the Web portal and Intranet servers will never be required to initiate a connection with any other system outside of the DMZ.

Task:

Create a set of rules (whitelist or blacklist) that fulfill the requirements set out above. Be sure to specify WHICH firewall has which ruleset.

Rules should be written in the order of execution and to save processing time as few rules should be used as possible. Marks will be awarded for accuracy and precision of the rule sets.

The Firewalls are NOT application aware so all communication protocols must be matched on port and direction alone.

Rules should take the form:

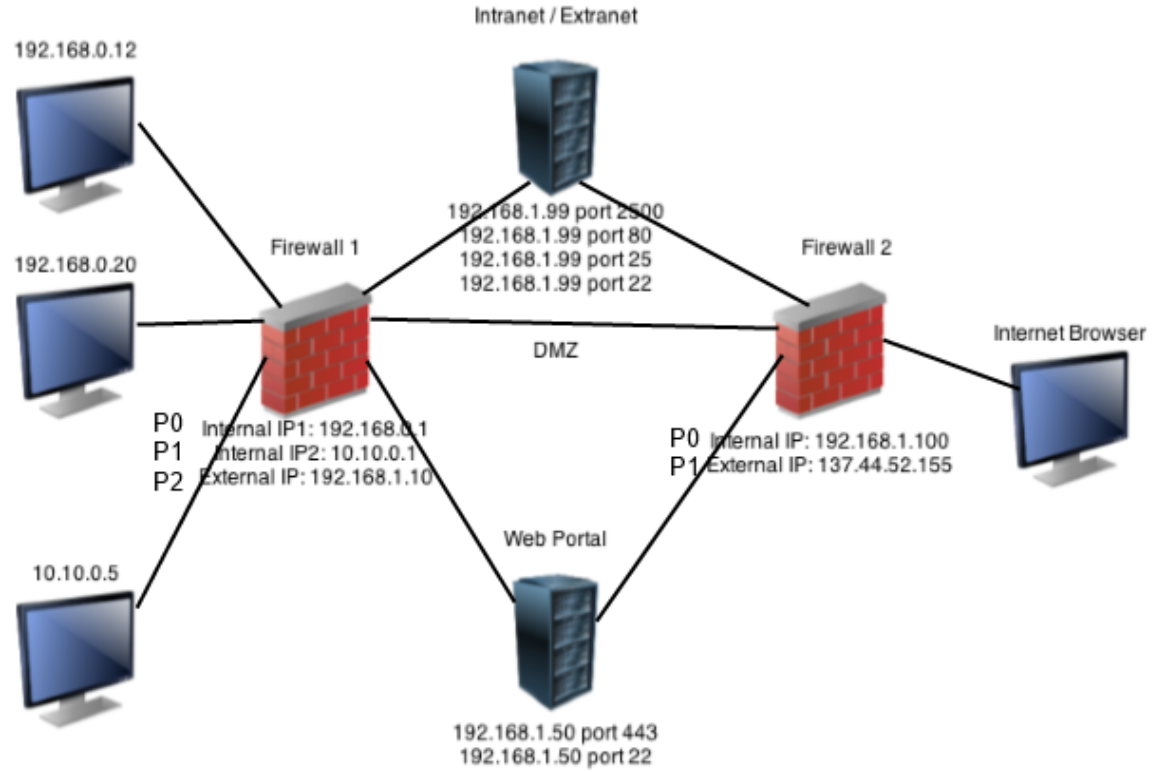
Firewall Port Source IP Direction Destination IP PORT ACTION

EG: firewall 1

Firewall Port Source IP: Direction Destination IP Port Action

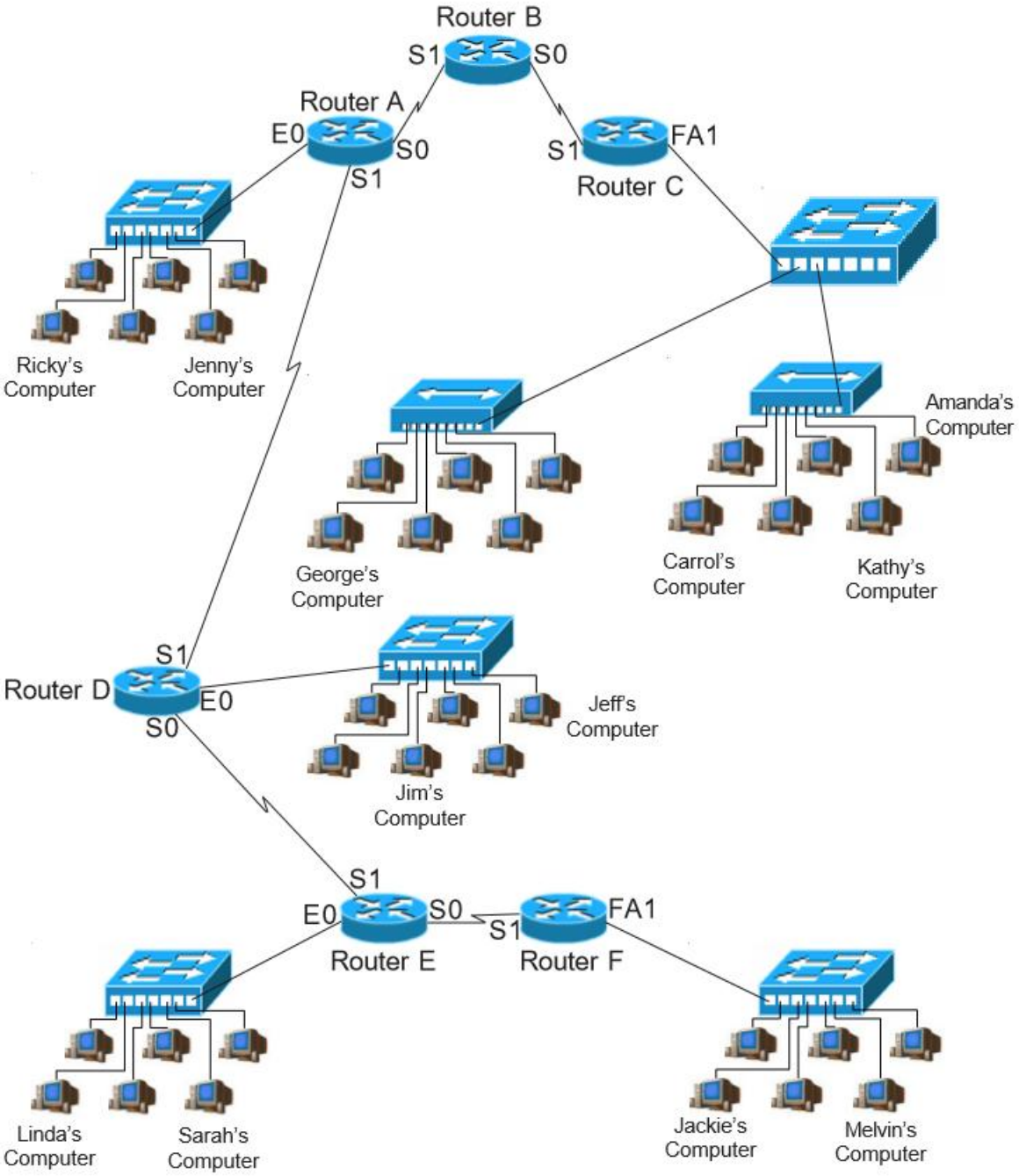
FW1:P1 10.10.0.0\24 OUT 192.168.1.99 ANY DENY

Systems Diagram:



Question 2: (20 marks)

Given the network diagram from the lecture on Access Control Lists:



Answer the following questions: (2 marks each)

1. Where would you place a standard access list to deny traffic to Carrol's computer from Sarah's computer?

2. Where would you place a standard access list to permit traffic from George's computer to reach Linda and Sarah's computer?

3. Where would you place an ACL to deny traffic from Jeff's computer from reaching George's computer?

4. Where would you place an extended access list to deny traffic to Sarah's computer from Jackie's computer?

5. Where would you place an extended access list to deny traffic to Jenny's computer from Sarah's computer?

6. Where would you place an extended access list to deny traffic from Linda's computer from reaching Jenny's computer?

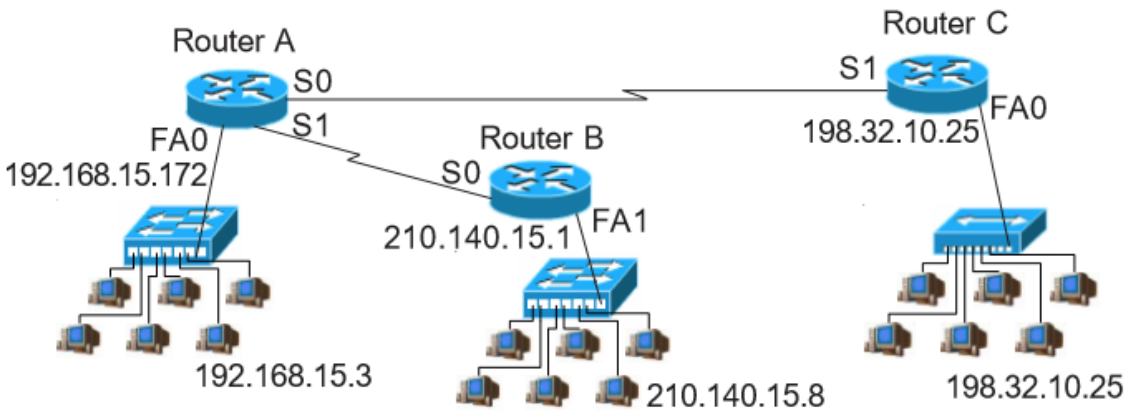
7. Create a wildcard mask to match this host. IP Address: 195.190.10.35 Subnet Mask: 255.255.255.0

8. Create a wildcard mask to match this range. IP Address: 10.0.0.0 Subnet Mask: 255.0.0.0

9. Create a wildcard mask to match this range. IP Address: 210.150.28.16 Subnet Mask: 255.255.255.248

10. Create a wildcard mask to match this range. IP Address: 172.18.0.0 Subnet Mask: 255.255.224.0

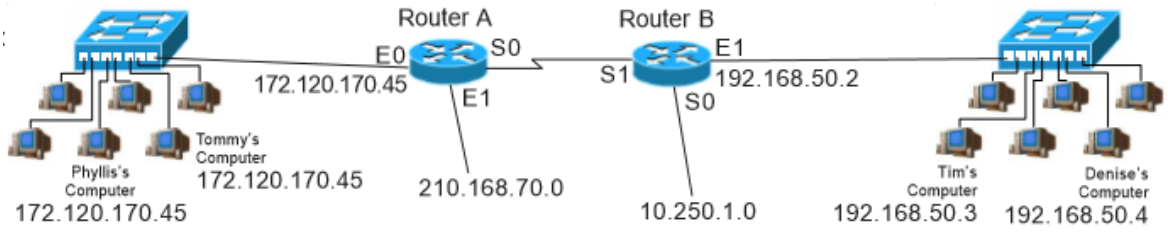
Question 3: (10 marks) Given the following network map:



Write a standard access list to block the addresses 192.168.15.1 to 192.168.15.31 from sending information to the 210.140.15.0 network. Do not permit any traffic from 198.32.10.25 to reach the 210.140.15.0 network. Permit all other traffic. You must state where you are placing the ACL and what your ACL number will be. Keep in mind that an ACL may consist of more than one permit or deny statement.

Question 4: (15 marks)

Given the following network map:



Write a named extended access list called "Godzilla" to prevent the 172.120.0.0 network from sending information to the 210.168.70.0 , and 10.250.1.0 255.255.255.0 networks; but will permit traffic to the 192.168.50.0 network. Permit all other traffic. Keep in mind that there may be multiple ways many of the individual statements in an ACL can be written and your list may require more than one permit or deny statement.

Question 5: (25 marks)

Write a brief report (between 1 and 2 pages - 500 to 1000 words) that compares RADIUS to TACACS (or TACACS+) and identifies which circumstances would lead to one system being preferrable to another. You must provide at least 5 links, none of which may be from wikipedia or linked as external resources on the wikipedia pages for either of the systems.

Your links will be scored based on their authority (strongest to weakest are: academic papers , technical whitepapers , manufacturer/owner instructions , technical blogs , user opinion blogs , non-technical forum posts).