CS 640 Introduction to Computer Networks

Quiz 4

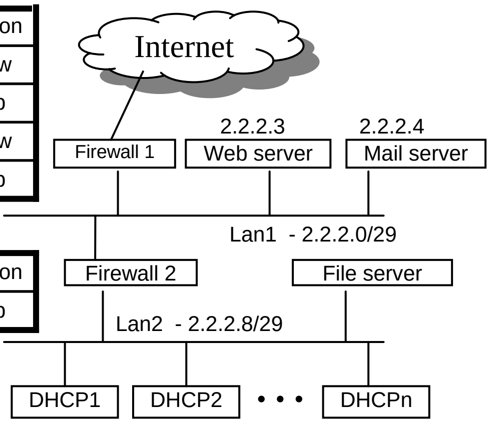
Write your name on the exam. Write something for every question. Students who do not write something for everything lose out over students who write down wild guesses. You will get some points if you attempt a solution but nothing for a blank sheet of paper. Write something down, even wild guesses. Problems take long to read but can be answered concisely.

Question	Maximum	Score
1	12	
2	8	
Total	20	

Problem 2 – firewalls

srcIP	destIP	sPort	dPort	Proto	Action
*	2.2.2.3	*	80	TCP	allow
*	2.2.2.3	*	*	*	drop
*	2.2.2.4	*	25	TCP	allow
*	2.2.2.4	*	*	*	drop

srcIP	destIP	sPort	dPort	Proto	Action
*	2.2.2.8/29	*	*	TCP/SYN	drop



This is the firewall setup of a small company with a public web server, a mail server, a file server with confidential files and desktop computers using DHCP. The first table has the rules applied to incoming packets by firewall 1 and the second has the rules applied to incoming packets by firewall 2. Each packet is matched against the rules in the table in order and the first rule that matches applies. For example the first two lines drop all non-web traffic going to the web server. The rule in firewall 2's table blocks all incoming packets that only have the SYN flag set, thus making it impossible for outside computers to open TCP connections to computers behind the firewall, but allowing computers behind this firewall to initiate connections to outside computers.

a) Explain why they have two LANs and two firewalls, instead of just having all computers on one LAN and combining the two firewalls into one. Hint: imagine a malicious hacker with a web server exploit, and a file server exploit.

Assume firewall2 is not present. The attacker with the web server exploit can subvert the web server because firewall1 allows external users to connect to the web server. Now the attacker can launch an attack against the file server from the subverted web server. If firewall2 is in place this second attack is blocked and the attacker cannot get the confidential files.

b) What rule(s) would you need to add (and in which position) to firewall 1 to enable users to also check their email over IMAP (using port 143) from their home computers.

If the address of the IMAP server is 2.2.2.5 we need to insert (,2.2.2.5,*,143,TCP,allow) and (*,2.2.2.5,*,*,*,drop) in this order into any position in firewall1's ruleset.*

c) A security consultant proposes adding the rules (2.2.2.0/28,*,*,*,*,allow) and (*,*,*,*,*, deny) in this order to the rules applied to the outgoing packets by firewall1 (not shown in figure because the table is currently empty and passes all packets) to counter flooding DoS attacks with fake source addresses. Will this protect the company's computers from flooding attacks? How will these rules help?

This rule will not protect the company from DoS attacks, but if malicious hackers subvert computers from within this network they cannot use them to stage flooding attacks with fake source addresses. If the attackers use the actual source addresses of the computers they subverted, it is easier for the victim to filter the attack.

Question 2 – Tunneling

a) In mobile IP the packets the mobile node sends to the correspondent node need to be sent over the tunnel between the foreign agent and the home agent. Suppose the mobile node would send these packets directly. Why might this solution break in many settings?

If the network the mobile node is connected to uses egress filtering (filtering out packets that have source addresses outside the prefixes used by the network), these packets would get filtered out. If they are tunneled, the source address is that of the foreign agent so the packets go through.

b) Why is multicast traffic sent through tunnels in some cases?

Because not all routers support multicast and tunnels are needed to link multicast-enabled routers that are not directly connected.