Homework 3: Firewall Engineering

Kevin Jang (kj460)

COSC 435

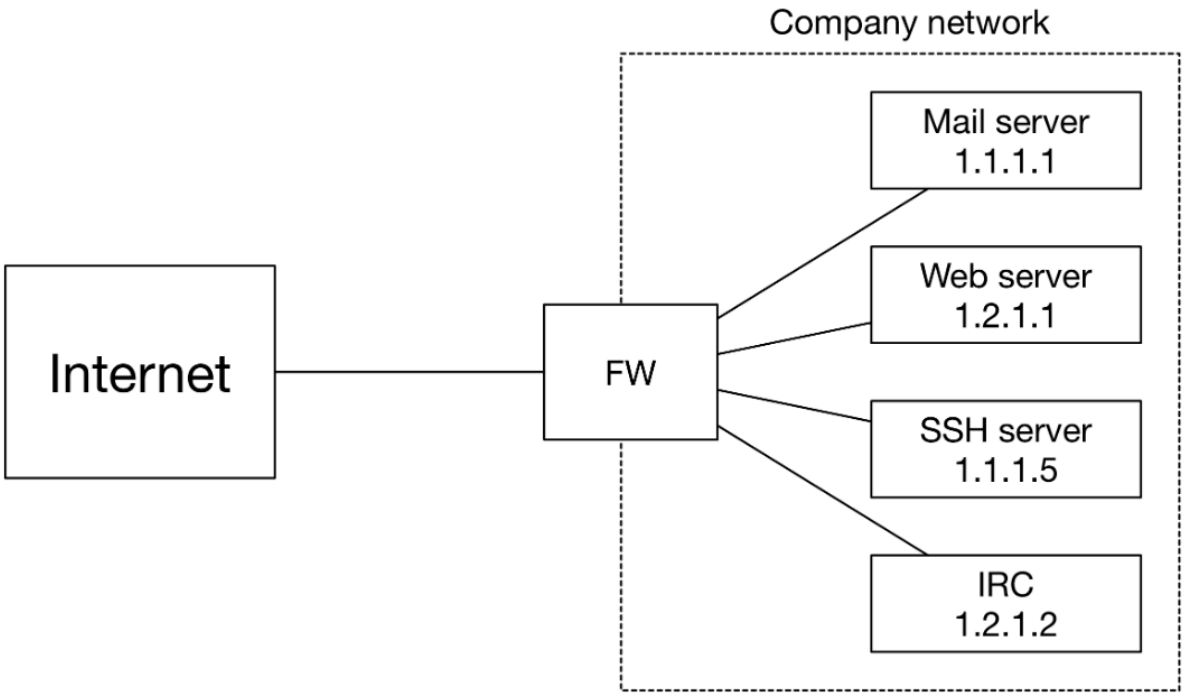
This homework is worth 40 points and contains no programming assignment. Homework solutions should be submitted as a single PDF to Autolab.

Assigned October 17, 2018; **due October 25th at 11:59pm**.

Written questions [40 points]

You have just been hired as a network security engineer for Saxa Saxs, an unpronounceable company that sells Georgetown-branded saxophones online. Congratulations!

The Saxa Saxs corporate network has the following structure:



As shown in the above figure, the corporate network consists of a mail server, a web server, an SSH server, and an IRC server. The IP addresses of the servers are shown in the figure. All servers use TCP. The ports used to receive incoming TCP connections is as follows:

Service	**TCP port (for incoming connections)**
Mail	25
Web	80 and 443 (for HTTP and HTTPS, respectively)
SSH	22
IRC	6667

Answers

Question 1 [26 points]. Complete the above firewall table/ruleset to enforce the above policies (and nothing else).

Your job is to protect the servers by configuring the firewall (identified as "FW" in the above figure). More specifically, your firewall should enforce the following policies (and nothing else):

- By default, all outgoing traffic should be allowed/accepted.
- Incoming traffic should be allowed to the mail server, but only if it is destined to the port used by the mail service.
- Incoming traffic should be allowed to the web server, but only if it is destined to the ports used by the web service.
- Incoming traffic should be allowed to the SSH server, but only if it is destined to the port used by the SSH service.
- Incoming traffic should be allowed to the IRC server, but only if it is destined to the port used by the IRC service.
- By default, all incoming network should be denied.

Note that *outgoing* traffic denotes traffic originating from inside the corporate network and destined for the Internet; *incoming* traffic denotes traffic originating from outside the corporate network and attempting to access a service inside the corporate network.

Rule#	Direction	Source IP	Source Port	Destination IP	Destination Port	Protocol	Action	Explanation
1	Outbound	*	*	*	*	TCP	Accept	Default allow rule for all outgoing traffic
2	Inbound	*	*	1.1.1.1	25	TCP	Accept	Allowing incoming traffic to the mail server that is destined to the mail server's port number (25)
3	Inbound	*	*	1.2.1.1	80	TCP	Accept	Allowing incoming traffic to the web server that is destined to the HTTP web server's port number (80)
4	Inbound	*	*	1.2.1.1	443	TCP	Accept	Allowing incoming traffic to the web server that is destined to the HTTPS web server's port number (443)
5	Inbound	*	*	1.1.1.5	22	TCP	Accept	Allowing incoming traffic to the SSH server that is destined to the SSH server's port number (22)
6	Inbound	*	*	1.2.1.2	6667	TCP	Accept	Allowing incoming traffic to the IRC server that is destined to the IRC server's port number (6667)
7	Inbound	*	*	*	*	TCP	Deny	Default deny rule for all incoming traffic

Question 2 [7 points]. Suppose that you detect a DoS attack originating from the network 5.4.3.x (or more formally, 5.4.3.0/24). What rule would you add to the firewall table you described above to block access from the 5.4.3.x network?

Location	Direction	Source IP	Source Port	Destination IP	Destination Port	Protocol	Action	Explanation
Before rule 2	Inbound	5.4.3.0/24	*	*	*	TCP	Deny	Denying incoming traffic from the IP address, 5.4.3.0/24 to block a DoS attack.

Question 3 [7 points]. The CEO of the company informs you that she does not want her employees accessing YouTube (IP address: 172.217.15.110) from work. What rule would you add to the firewall table you described **in question 1** to prevent your employees from connecting to 172.217.15.110?

Location	Direction	Source IP	Source Port	Destination IP	Destination Port	Protocol	Action	Explanation
Before rule 1	Outbound	*	*	172.217.15.110	*	*	Deny	Blocking all outgoing traffic to the IP address of YouTube (172.217.15.110)