Alivia Castor
Soc 11

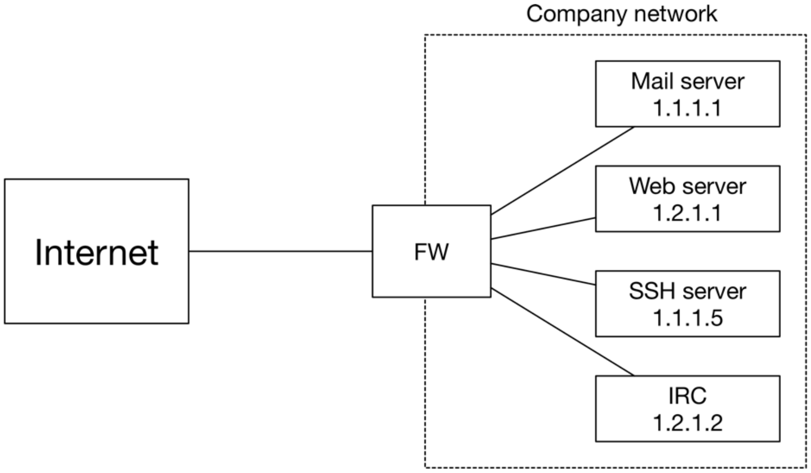
COSC4705 - Homework 4

This homework is worth 40 points and contains no programming assignment. Homework solutions should be submitted to Gradescope.

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:



Mail and SSH servers:
→ use addresses in the 1.1.1.x range
→ (1.1.1.1 and 1.1.1.5)

Web and IRC servers:
→ use addresses in the 1.2.1.x range
→ (1.2.1.1 and 1.2.1.2)

This grouping suggests that the internal network might be segmented into two subnets like (1.1.1.0|24 and 1.2.1.0|24)

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

Alivia Castor
Soc11

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.

Question 1 [25 points]. Complete the above firewall table/ruleset to enforce the above policies (and nothing else). Fill in the table below with rule #s matching the rules in order above.

Rule#	Direction (Inbound/Outbound)	Source IP	Source Port	Destination IP	Destination Port	Protocol	Action (accept/deny)	Explanation (free-form text)
1	Outbound	☆ 1.1.1.0/24; 1.2.1.0/24	*	0.0.0.0/0	*	TCP	accept	Permits all TCP traffic originating from any internal host (in both subnets) to any external destination. Subnets are assumed b/c of network diagram grouping (1.1.1.x and 1.2.1.x ranges).
2	Inbound	0.0.0.0/0	*	1.1.1.1	25	TCP	accept	Allows SMTP traffic only to the mail server (1.1.1.1).
3	Inbound	0.0.0.0/0	*	1.2.1.1	80,443	TCP	accept	Permits HTTP/HTTPS traffic (ports 80 and 443) exclusively to the web server (1.2.1.1).
4	Inbound	0.0.0.0/0	*	1.1.1.5	22	TCP	accept	Permits SSH traffic (port 22) only to the SSH server (1.1.1.5).
5	Inbound	0.0.0.0/0	*	1.2.1.2	6667	TCP	accept	Allows IRC traffic (port 6667) soley to the IRC server (1.2.1.2).
6	Inbound	0.0.0.0/0	*	0.0.0.0/0	*	TCP	deny	Blocks any inbound TCP traffic not explicitly allowed by rules 2-5.

☆ Here I choose to divide the network into subnets (based on the network diagrams grouping (1.1.1.0/24 for Mail/SSH and 1.2.1.0/24 for web/IRC). I choose this over using one supernet (like 1.0.0.0/16) b/c using subnets is more secure and allows us to apply precise firewall rules for each group to isolate any potential breaches and reduce unnecessary broadcast traffic (can't do these things w/ one large supernet).

You must use CIDR notation to denote network ranges (e.g., 0.0.0.0/0 denotes "all hosts on the Internet" or "any IP"). In the second column ("Direction"), specify either "Inbound" or "Outbound" to denote whether the rule applies to traffic entering or exiting the network, respectively. For ports, specify by number or * for all.

Please provide a **brief** explanation as to the purpose of each rule in the right-most column.

Your solution should not make any assumptions about whether the firewall has a default-accept or default-deny policy.

Alivia Castor
soc11

Question 2 [5 points]. Suppose that you detect a DoS attack originating from the network 5.4.3.0/24. What rule would you add to the firewall table you described above to block access from the 5.4.3.0/24 network?

Location	Direction (Inbound/Outbound)	Source IP	Source Port	Destination IP	Destination Port	Protocol	Action (accept/deny)	Explanation (free-form text)
Before rule 2 in the inbound Chain	Inbound	5.4.3.0/24	*	0.0.0.0/0	*	TCP	deny	Immediiatly drops all TCP traffic from the 5.4.3.0/24 network to block the DoS attacking network. Thus, preventing it from matching/ Processing any later allow rules.

Please be precise as to where the rule should be inserted -- e.g., write "before rule 2" in the Location column if this new rule should be inserted before rule 2 as described in the table from Question 1.

Question 3 [5 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 (Inbound/Outbound)	Source IP	Source Port	Destination IP	Destination Port	Protocol	Action (accept/deny)	Explanation (free-form text)
Before Rule 1 in the outbound chain	Outbound	1.1.1.0/24; 1.2.1.0/24	*	172.217.15.110/32	*	* TCP	deny	Prevents any outbound TCP connection from any corporate hosts (both Subnets) to YouTube's IP address.

Subnets of the network (1.1.1.x and 1.2.1.x).

Please be precise as to where the rule should be inserted -- e.g., write "before rule 2" in the Location column if this new rule should be inserted before rule 2 as described in the table from Question 1.

Question 4 [5 points]. You realize that the IRC server is likely to be compromised, and you would like to isolate the IRC server from other internal systems. Assuming that all servers communicate through the firewall, what rule would you write that would prevent the IRC server from communicating with the other severs?

Location	Direction (Inbound/Outbound)	Source IP	Source Port	Destination IP	Destination Port	Protocol	Action (accept/deny)	Explanation (free-form text)
Before any rule that permits inter-server communications	Outbound	1.2.1.2	*	1.1.1.0/24; 1.2.1.0/24	*	* TCP	deny	Block all outbound traffic from the IRC server (1.2.1.2) to any internal server, thus isolating it from the corporate network.

subnets of the network w/ subsets grouped like (1.1.1.x and 1.2.1.x).

Alivia Castor
soc 11

Please be precise as to where the rule should be inserted -- e.g., write "before rule 2" in the Location column if this new rule should be inserted before rule 2 as described in the table from Question 1.

Submission Instructions

Please submit your solution as a PDF via Gradescope.

Please post questions (especially requests for clarification) about this homework to Ed.