Hacettepe University Computer Engineering
BBM 465 Information Security Laboratory

46th Group

December 2020

1 Instruction

What is Firewall
Firewall is a security device that monitors all network traffic on selected devices (what we mean is devices which use firewall). Based on devices' purposes/rules, data packages which is incoming or outgoing can be blocked or permitted via firewall. With blocking/permitting operations, device is protected from unauthorized (it can be a virus, a trojan or a hacker)/unwanted access from outside by firewall, which makes devices more secure. [1]
It's like the air conditioner filters the air which enters from the outside of the home (all requests), dusts and some gases(unwanted/unauthorized access) can not pass the filter but some gases passes, then air conditioner sends the fresh (or filtered, known/authorized access) air to the room.

What is Iptables
Iptables is the filter of IP addresses, packets or MAC addresses. Iptables is used to make firewall rules, which sources can be accepted or dropped/ which destination addresses that can be sent / which interfaces are allowed/disallowed etc. In one iptables file, different tables are defined, and each table contains a number of built-in chains and may also contain user-defined chains.

Iptables Chains
Chains are like a storage for different iptables rules. Many rules can be defined in chains. There may be some built-in chains but you can create custom chains. [2] Chains are based on which table is selected (for example, default table is filter table, we have three chains : INPUT, OUTPUT and FORWARD), rules are added to chains based on the argument value. Also in every chain, rules are applied by different ways in different sections, for example INPUT chain permits/blocks incoming data but OUTPUT chain permits/blocks outgoing data In every chain, there is a list of rules which can match a set of packets. Each rule specifies what to do with a packet that matches. This is called a 'target', which may be a jump to a user-defined chain in the same table.[3]

Solution Approach

In every question, our default policy was drop in order to achieve what the question asks. We used similar approaches in these questions. In firewall device, forward keyword are used many times for establishing communication between intended interfaces. Input and Output chains are used by local machines/servers. We used range for specifying Computer Engineering, Electronic Engineering and Physics Engineering machines' IP addresses. [4] [5] [6]

2 Question 1

Firstly, we need to define iptables rules in Computer Engineering and Electroinc Engineering. Our default policy is drop everything except specified ip addresses. After that, we added some rules that input can be sent from Computer Engineering Ip addresses in Computer Engineering section (Electronic Engineering Ip addresses in Electronic Engineering) (in order to apply this, we need ip range) and output can be accepted from Electronic Engineering (Computer Engineering in Electronic Engineering section), port number wasn't written on question but in figure we saw port 24. Also in internet, we saw that port 24 is used for private mail. Thus we used port 24 for communication.

For communication, both machines must be on same port(24) and these machines both receives(incoming) and transmits(outgoing) data.

In Firewall, our default policy is drop everything except specified interfaces, we added them. After that, we added some rules that can permit communication between two interfaces, eth1 and eth2. After these rules are defined, we saved iptables rules.

3 Question 2

In question 2, iptables rules use ports 80(HTTP) and 443(HTTPS) , which will be used for the question. Since iptables default policy is drop everything except specified ip addresses which is defined in iptables_2 file, iptable drops other connection if source argument connection is not lan1(Computer Engineering), lan2(Electronic Engineering), lan3(Physics Engineering) computers and destination argument is not Twitter and Youtube servers. In firewall device, our default policy is drop everything except specified interfaces. With applying this policy, interfaces except eth1, eth2, eth3 and eth4 are dropped. Also, we added extra rule for eth4. We don't want to communication between any machine to remote server. Thus we added a rule that blocks remote server from eth4.

4 Question 3

In question 3, outside of campus means, any ip address. Thus we accepted ip addresses from anywhere(0/0) on servers which is defined in web server and e-mail server. We used 80(HTTP) and 443(HTTPS) ports for web server and 25(SMTP) port for e-mail server.
In firewall our default policy is drop everything except specified interfaces (we use this policy again because any ip address which is outside of the campus doesn't need to use firewall, it can communicate directly to the web server and e-mail server), We added extra rule for eth4. Because we don't want to communication between any machine to Youtube and Twitter. Thus we added a rule that blocks Youtube and Twitter from eth4.

5 Question 4

In question 4 our default policy is drop everything except specified ip addresses, iptables rules use ports 110(POP3) and 143(IMAP4) , which will be used for the question. Since iptables default policy is defined in iptables_4 file, iptable drops other connections if connection source is not lan1(Computer Engineering), lan2(Electronic Engineering), lan3(Physics Engineering) computers and destination argument is not Mail server. We added these rules and saved it.
In firewall device our default policy is drop everything except specified interfaces again., interfaces except eth1, eth2, eth3 and eth0 are dropped. Also we don't want to communication between any machine to web server. Thus we added a rule that blocks web server from eth0. We added the rules as we mentioned, then saved it.

6 Question 5

In iptables rules, our default policy is drop everything except specified ip addresses again. Also icmp protocol is used.
Incoming devices such as lan1, lan2, lan3 are using echo-request icmp type for Input and echo-reply icmp type for Output.
Outgoing device such as Remote Computer is using echo-reply icmp type for Input and echo-request icmp type for Output.
In firewall device, our default policy is drop everything except specified interfaces again, interfaces except eth1, eth2, eth3 and eth4 are dropped.
Also, we added extra rule for eth4. Because we don't want to be pinged from youtube and twitter. Thus we added a rule that blocks youtube and twitter from eth4. Then all rules are saved.

7 Question 6

In question 6 our default policy is drop everything except specified ip addresses but one difference here: there is a connection limit. In order to avoid DDoS attack (max 100 connections at the same time), iptable rule uses connlimit argument (and set to above 101) [7]
Iptables rules use port 443(HTTPS). Since iptables default policy is defined in iptables_6 file. Iptable drops other connection if connection source is not lan1(Computer Engineering), lan2(Electronic Engineering), lan3(Physics Engineering) computers, connection destination is not Twitter and Youtube servers. We added rules as we mentioned earlier, then saved it.
Also in firewall device our default policy is drop everything except specified interfaces. With applying this policy,interfaces except eth1, eth2, eth3, eth4 and eth0 are dropped , we don't want to make any communication between any machine to youtube and twitter. Thus we added a rule to firewall that blocks youtube and twitter from eth4.

8 References

- https://www.forcepoint.com/tr/cyber-edu/firewall
- https://blog.sleeplessbeastie.eu/2018/06/21/how-to-create-iptables-firewall-using-custom-chains/
- https://linux.die.net/man/8/iptables
- http://www.iptables.info/
- http://www.thegeekstuff.com/2011/06/iptables-rules-examples/
- http://www.cyberciti.biz/tips/linux-iptables-examples.html
- https://javapipe.com/blog/iptables-ddos-protection