

HACETTEPE UNIVERSITY

DEPARTMENT OF COMPUTER ENGINEERING

BBM465 – Information Security Laboratory

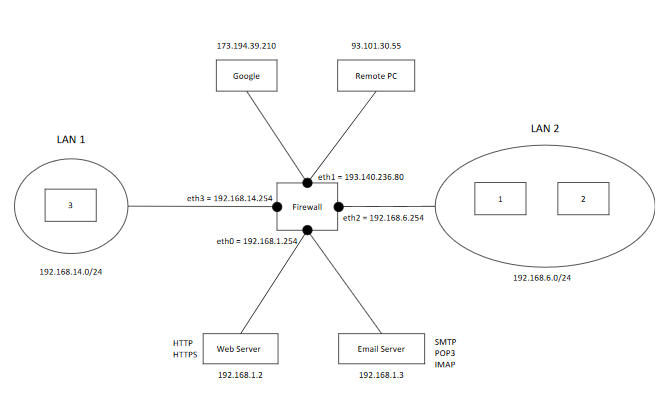
Students: Mümin Can Yılmaz – Hayati İbiş – İrem Özen

Subject: Firewall

**INTRODUCTION**

In this experiment, we are expected to configure the specific network’s firewall via iptables.

Network;



There are specific configurations that given from instructors. These configurations are;

1. Write the necessary configurations so that computer 1 can ping only to computer 3.

2. Write the necessary configurations so that computer 3 can ping all of the computers in LAN 1 (Note: This will be done using ipset).

3. Write the necessary configurations so that remote PC can only access Web Server and Email Server.

4. Write the necessary configurations so that the computers on LAN 1 and LAN 2 can only access the Google machine.

5. Write the necessary configurations so that no more than 7 computers can access the Web Server at the same time (Note: Configuration will be done on Firewall, not Web Server).

6. Write the necessary configurations so that the Firewall can be accessed via ssh from port 40000 (Note: ssh connection must be opened when we write ”ssh 193.140.236.80 –p 40000” command to the console).

**CONFIGURATIONS**

**Configuration – 1 : Write the necessary configurations so that computer 1 can ping only to computer 3.**

First of all, we don’t know the specific ip addresses of computer 1 and computer 3. So, we need to adjust the firewall via eth’s ip addresses.

*iptables -A OUTPUT -s 192.168.6.254 -d 192.168.14.254 -j ACCEPT*

With this command we allow eth2 to send packets to eth3.

*iptables -A INPUT -s 192.168.6.254 -d 192.168.14.254 -j ACCEPT*

And with this command we allow eth3 to accept packets from eth2.

**Configuration – 2 : Write the necessary configurations so that computer 3 can ping all of the computers in LAN 1 (Note: This will be done using ipset).**

First, we need to use the ipset command to create a set of ips. Also like the configuration 1 we again don’t know the specific ip address of computer 3.

|  |
| --- |
| *ipset -N LAN1 iphash* |
|  |

|  |
| --- |
| *ipset -A 192.168.14.0* |
|  |

|  |
| --- |
| *ipset -A 192.168.14.1* |
|  |

*ipset -A 192.168.14.2 …*

Now, we need to allow eth3 to send packets to LAN1.

*iptables -A OUTPUT -m set --set LAN1 dst -s 192.168.14.254 ACCEPT*

Then, we are going to allow the computers from LAN1 to accept the packets from computer3.

*iptables -A INPUT -m set --set LAN1 dst -s 192.168.14.254 ACCEPT*

**Configuration – 3 : Write the necessary configurations so that remote PC can only access Web Server and Email Server.**

First, we are going to write the configurations for remote PC. Now, we are going to allow remote PC to send packets to email server and web server.

*iptables -A OUTPUT -s 93.101.30.55 -d 192.168.1.3 -j ACCEPT*

*iptables -A OUTPUT -s 93.101.30.55 -d 192.168.1.2 -j ACCEPT*

Now, we are going to allow remote PC to take packets from email server and web server.

|  |
| --- |
| *iptables -A INPUT -s 192.168.1.3 -d 93.101.30.55 -j ACCCEPT* |
|  |

|  |
| --- |
|  |

|  |
| --- |
| *iptables -A INPUT -s 192.168.1.2 -d 93.101.30.55 -j ACCCEPT* |
| Now, going to configure the email server and web server so, the email server and web server can send and receive packets from remote PC.  Email server ;   |  | | --- | | *iptables -A INPUT -s 93.101.30.55 -d 192.168.1.3 -j ACCEPT* | |  |  |  | | --- | |  |  |  | | --- | | *iptables -A OUTPUT -s 192.168.1.3 -s 93.101.30.55 -j ACCEPT* | |  | |  | |
|  |

Web Server;

|  |
| --- |
| *iptables -A INPUT -s 93.101.30.55 -d 192.168.1.3 -j ACCEPT* |
|  |

|  |
| --- |
|  |

|  |
| --- |
| *iptables -A OUTPUT -s 192.168.1.3 -s 93.101.30.55 -j ACCEPT* |
| Thus, remote PC now can talk with both email server and web server. |
|  |

**Configuration – 4 : Write the necessary configurations so that the computers on LAN 1 and LAN 2 can only access the Google machine.**

First, we are going to allow LAN1 to send and receive packets from Google machine.

|  |
| --- |
| *iptables -A OUTPUT -s 192.168.14.0/24 -d 173.194.39.210 -j ACCEPT* |
|  |

|  |
| --- |
|  |

|  |
| --- |
| *iptables -A INPUT -s 173.194.39.210 -d 192.168.14.0/24 -j ACCEPT* |
| Then, we are going to configure LAN2 to do the same.   |  | | --- | | *iptables -A OUTPUT -s 192.168.6.0/24 -d 173.194.39.210 -j ACCEPT* | |  |  |  | | --- | |  | |  |  |  | | --- | | *iptables -A INPUT -s 173.194.39.210 -d 192.168.6.0/24 -j ACCEPT* | |  | |
|  |

Now, we are going to allow google machine to send and receive packets from LAN1 and LAN2.

|  |
| --- |
| *iptables -A OUTPUT -s 173.194.39.210 -d 192.168.14.0/24 -j ACCEPT* |
|  |

|  |
| --- |
|  |

|  |
| --- |
| *iptables -A OUTPUT -s 173.194.39.210 -d 192.168.6.0/24 -j ACCEPT* |
|  |

|  |
| --- |
|  |

|  |
| --- |
|  |
|  |

|  |
| --- |
| *iptables -A INPUT -s 192.168.14.0/24 -j ACCPET* |
|  |

|  |
| --- |
|  |

|  |
| --- |
| *iptables -A INPUT -s 192.168.6.0/24 -j ACCPET* |
|  |

Thus, now the computers at LAN1 and LAN2 can talk to Google machine.

**Configuration – 5 : Write the necessary configurations so that no more than 7 computers can access the Web Server at the same time (Note: Configuration will be done on Firewall, not Web Server).**

At the part, we are going to configure the firewall, so that it won’t allow no more then 7 computers to access the Web server at the same time.

First, we are going to reject the connections where connection number is more then 7.

*iptables -A INPUT -d 93.101.30.55 -m state --state NEW -m connlimit --connlimit-above 7 -j REJECT*

*iptables -A OUTPUT -s 93.101.30.55 -m state --state NEW -m connlimit --connlimit-above 7 -j*

*REJECT*

Now, we are going to tell the firewall to accept the packets from computers that already established a connection with web server.

|  |
| --- |
| *iptables -A INPUT -d 93.101.30.55 -m state --state ESTABLISHED,RELATED -j ACCEPT* |
|  |

*iptables -A OUTPUT -s 93.101.30.55 -m state --state ESTABLISHED,RELATED -j ACCEPT*

Now, the web server will send and receive the packets from computers which established a connection. But at the same time, the web server won’t be able to accept new connection if the established connection number is more then 7.

**Configuration – 6 : Write the necessary configurations so that the Firewall can be accessed via ssh from port 40000 (Note: ssh connection must be opened when we write ”ssh 193.140.236.80 –p 40000” command to the console).**

Now, we are going to write the commands to configure the ssh connection to firewall.

First, we are going to allow firewall to accept a new ssh connection over port 40000.

*iptables -A INPUT -p tcp -d 193.140.236.80 --sport ssh --dport 40000 -m state --state NEW,ESTABLISHED -j ACCEPT*

Now, we are going to allow to send packets back to connections which is established.

*iptables -A OUTPUT -p tcp -s 193.140.236.80 --sport 40000 --dport ssh -m state --state ESTABLISHED -j ACCEPT*

**RESOURCES**

1. <https://www.howtogeek.com/177621/the-beginners-guide-to-iptables-the-linux-firewall/>
2. <https://www.cyberciti.biz/faq/rhel-fedorta-linux-iptables-firewall-configuration-tutorial/>
3. <https://serverfault.com/questions/371316/iptables-difference-between-new-established-and-related-packets>
4. <http://www.linuxjournal.com/content/advanced-firewall-configurations-ipset>
5. <https://unix.stackexchange.com/questions/139285/limit-max-connections-per-ip-address-and-new-connections-per-second-with-iptable>
6. <http://ipset.netfilter.org/iptables-extensions.man.html>
7. http://www.iptables.info/en/connection-state.html