

## eh1act05 – Firewalls

### GENERAL CONDITIONS

#### 1- Deadline:

- DAW1: **4-5-26**
- ASIX1: **30-4-26**

2- Teacher will check that your operating system is working properly

### DOCUMENTATION

#### 1- Basic ideas

A **firewall** is a security system that monitors and controls **incoming and outgoing network traffic** based on **predetermined security rules**. It acts like a **barrier** between a trusted network (like your home or office network) and an untrusted one (like the internet).

A firewall performs tasks such as:

- **Blocking unauthorized access** to or from a private network.
- **Monitoring traffic** for suspicious activity.
- **Allowing safe communication** between trusted systems.
- **Preventing malware** and hackers from accessing your system.

A firewall should be used in order to:

- To **protect personal or organizational data**.
- To **control employee access** to certain websites.
- To **create secure connections** (especially important for remote work).
- To **comply with regulations** like [General Data Protection Regulation](#) (also called GDPR).

There are different types of firewall but, on most personal computers, users install a **Packet-Filtering firewall** that is a software that **filters** data based on **IP addresses, ports, protocols** or **direction (inbound or outbound)** of traffic.

A **Packet-Filtering** firewall works with **rules**. These rules are a **set of instructions** that tell a Packet-Filtering firewall what traffic to **allow** or **block** based on IP addresses, ports, protocols or direction of traffic.

**UFW** (Uncomplicated Firewall) It's a **user-friendly** software for **managing** firewall **rules** on **Linux** systems. It makes setting up a firewall **simple** and **quick**, even for beginners.

#### 2- Installing, managing and monitoring UFW

- a) Installation → **sudo aptitude install ufw**
- b) Enabling UFW → **sudo ufw enable**
- c) Disabling UFW → **sudo ufw disable**
- d) Disabling and resetting firewall to installation defaults → **sudo ufw reset**

**NOTE 1:** If you enable UFW, it is started immediately and it will be started during the boot process.

**NOTE 2:** If you disable UFW, it is stopped immediately and it will not be started during the boot process.

**NOTE 3:** By default, all incoming traffic is blocked

**NOTE 4:** By default, all outgoing traffic is allowed.

#### 3- Monitoring UFW

- a) Show status and default setting of UFW → **sudo ufw status verbose**
- b) Show all active rules with index numbers → **sudo ufw status numbered**

#### 4- Adding and removing a basic rule to filter connections to a specific port of your computer

a) A typical firewall rule protects your computer by blocking connections to a specific port from all sources, except for one or a group of explicitly allowed computers.

If you want to adding a rule to **DENY** traffic to an specific port number of your computer from all sources, except for one allowed computer run the following commands:

```
sudo ufw allow from <IP address> to any port <Port number>
sudo ufw deny <Port number>
```

where:

- **<Port number>** is a port of your computer.
- **<IP address>** is the IP address of another computer allowed to connect to port 22 of your computer

b) Example:

```
sudo ufw allow from 192.168.1.100 to any port 3306
sudo ufw deny 3306
```

**blocks incoming connections** to **port number 3306** of your computer (typically used by MySQL) allowing access only from **192.168.1.100**.

**Order matters** → UFW processes rules top to bottom and stops at the first match. The allow rule for **192.168.1.100** must come **before** the deny rule, otherwise all traffic will be denied first.

c) If you want to remove the rules:

- Firstly, show all active rules with index numbers (check command in section 3).
- Secondly, find the rule you want to remove and its index number
- Finally, remove the rule → **sudo ufw delete [rule number]**

d) Example:

- Show all active rules with index numbers → **sudo ufw status numbered**
- **Status: active**

	To		Action	From
	--		-----	----
[ 1]	3306	(from 192.168.1.100)	ALLOW IN	192.168.1.100
[ 2]	3306		DENY IN	Anywhere
[ 3]	3306	(v6)	DENY IN	Anywhere (v6)

I want to remove rules 1 to 3.

- **sudo ufw delete 3**  
**sudo ufw delete 2**  
**sudo ufw delete 1**

**Why reverse order?** When you delete rule 1, rules 2 and 3 shift up and become rules 1 and 2. Deleting from the bottom up avoids this problem.

## **5- Basic rules to deny ping to your computer**

a) Another typical firewall rule is to protect your computer by blocking ping requests. If you want to do so, follow this steps:

- First of all, edit the UFW "before rules" file: **sudo nano /etc/ufw/before.rules**
- Secondly, find the section **#ok icmp codes** (lines 33 to 43).
- Thirdly, comment any line related to **icmp**.
- Fourthly, save **/etc/ufw/before.rules** and exit.
- Finally, reload UFW:  
**sudo ufw disable**  
**sudo ufw enable**

b) If you want to allow pings again you have to undo the previous steps and run again the commands to disable an enable **ufw**.

## **PRACTICAL EXERCISE**

### **PART 1**

- 1- Install and enable UFW on your virtual machine. Check the UFW status
- 2- Start service **apache** on your computer. Check the **port** opened by **apache**.
- 3- Creates a new **index.html** on your virtual computer that displays your name and group (asix1 or daw1).
- 4- Check the IP address of your physical computer.
- 5- **Allow only** your physical computer to access **apache service** on your virtual machine.
- 6- **Show** the rules of UFW.
- 7- Check:
  - That your physical computer can access to apache service and that index.html is displayed.
  - Another computer can not access apache service and that index.html is not displayed.

### **PART 2**

- 1- **Deny pings** to your virtual machine.
- 2- Check from your physical computer that pings requests are not answered by your virtual machine.

### **PART 3**

- 1- Reset UFW
- 2- Check that UFW is disabled and it has been reseted to installation defaults.

## **CHECKING YOUR SYSTEM**

- 1- Show the rules of UFW.
- 2- Verify that your physical computer can access the Apache service and that index.html file is displayed.
- 3- Verify that other computers cannot access the Apache service and that the index.html file is not displayed.
- 4- Verify from your physical computer that ping requests are not answered by your virtual machine.
- 5- Reset UFW and verify that it is disabled and restored to its installation defaults.