

# Public WLAN

## 1. Objectives

The objectives of this practical work are:

- a) Understand how a public WLAN infrastructure can be setup
- b) Understand how DHCP and DNS
- c) Verify the operation of a captive portal
- d) Verify how performance throttling works
- e) Usage of virtual machines and their interconnection with other virtual/physical Links

## 2. Introduction

This execution of practical work will guide through the setup, configuration and usage of a Captive Portal to control a Firewall, which provides access to external networks. pfSense provides a free implementation of two components. To emulate a WLAN hotspot an Access Point, implemented by a laboratory Fiber Gateway, will be used.

### a. Duration

This work is expected to take one class, practical component (1h15)

### b. Equipment

This work will use, per group:

- 1) 1x Fiber Gateway (AP)
- 2) 1x laboratory PC, with Linux (Ubuntu)
- 3) 1x student terminal with WLAN/802.11 interface
- 4) 2x Virtual Machines (VM) to:
  - a. Run pfSense Server
  - b. Run a configuration machine, in the management network

### c. Network diagram

Your laboratory PC already has VirtualBox installed and you will find two VM in the Desktop.

The first VM ('pfSense Server') is already installed with pfSense that implements a Firewall controlled by a Captive Portal, often used to control access to Internet when connect to in public and private spaces hotspots via WLAN accesses. A second VM ('pfSense Config') is used to access the pfSense configuration web page via an internal VirtualBox network ('Vboxnet0').

The pfSense Server connects (Adaptor 3, bridged to an ethernet interface of the lab PC) to an AP (implemented by a Fiber Gateway), providing controlled access

(via Adaptor 1, also bridged to an ethernet interface of the lab PC) to external networks (e.g. Internet).

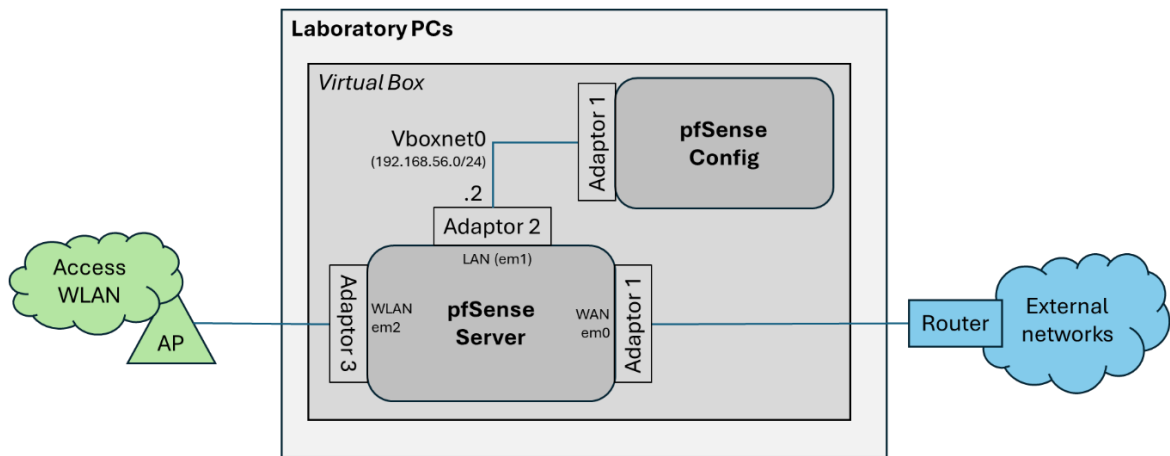


Figure 1: Reference network diagram

When connecting your WLAN devices to the AP, you shall get the following configuration:

- IP Address: 192.168.57.0/24
- Gateway: 192.168.57.2
- DNS Servers: 193.136.172.20 193.136.172.21 (DNS of the UA)

The pfSense Config VM shall get the following configuration:

- IP Address: 192.168.56.0/24
- Gateway: 192.168.56.2

To carry out the tests, use the following users in the Captive Portal:

Users	Pass.	Speed Download /Upload (kbps)	Time (minutes)	Traffic Volume Download /Upload (MB)	Associated test URL
cm	cm	unlimited	unlimited	unlimited	<a href="https://www.nperf.com/en/">https://www.nperf.com/en/</a>
cm_band	cm	1024/128	unlimited	unlimited	<a href="https://www.nperf.com/en/">https://www.nperf.com/en/</a>
cm_time	cm	unlimited	2	unlimited	any
cm_traffic	cm	unlimited	unlimited	16	<a href="https://www.gns3.com/software/download-vm">https://www.gns3.com/software/download-vm</a>

Table 1: Configured test users

For more information on pfSense, use the URL links in 'References' section, at the end.

### 3. Initial physical network setup

1. Get one Ethernet USB Adapter and an Ethernet cable from the laboratory
2. Connect the USB Ethernet Adapter to a USB 3 port (blue color) in the back of the Lab PC
  - **DO NOT CONNECT THE ETHERNET CABLE YET**
3. Open a 'Terminal Emulator' in the Lab PC and run the command 'ifconfig'
  - A new ethernet interface named 'enxMMMMMMMMMMMMMM' shall be present, where 'MMMMMMMMMMMMMM' is the MAC address of this interface (compare it with the 'ether' field)
4. Switch on the Fiber Gateway

### 4. pfSenseServer VM VirtualBox installation

5. In your lab PC Desktop, check the existence of two .ova files corresponding to the two VMs you are going to use in this practical exercise:
  - a) *pfSenseServer.ova*: image of the VM that will run the pfSense server, central piece of the experiment you going to carry out;
  - b) *pfSenseConfig.ova*: image of the auxiliary VM that will be used to access the pfSense server configuration and status.
6. Double click in the 'pfSenseServer.ova' VM image; VirtualBox (VBox) shall start with the following window (Figure 3); press 'Import'.

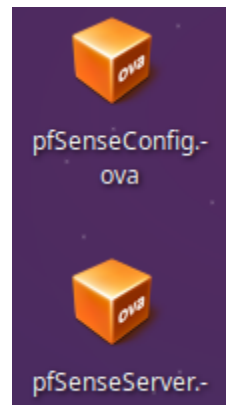


Figure 2: VM images to be used

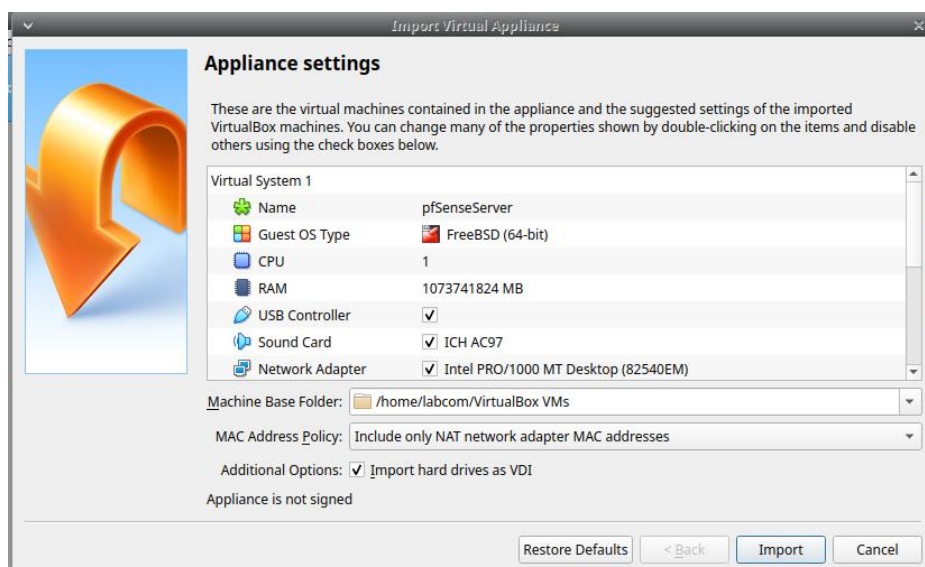


Figure 3: Virtualbox Config

7. When finished, in VBox 'Tools', select 'Network'

- a) If there any network configured, 'Remove' it;
- b) 'Create' a new network (shall be named 'vboxnet0' automatically) and unselect 'DHCP' server; *IP addresses will be assigned by the pfSense server*;
- c) Take note of the IP network associated to this VBox internal network.

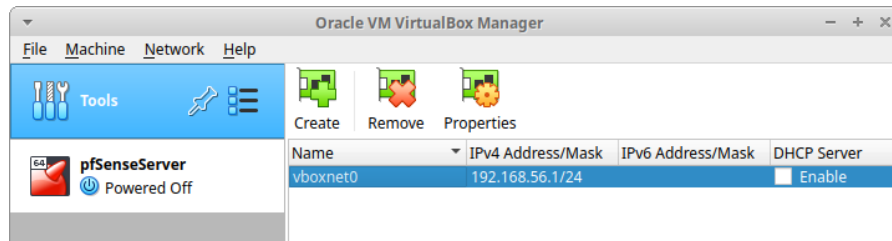


Figure 4: VirtualBox internal network creation

8. Go to the 'Settings' of the recently created VM ('pfSenseServer') and select 'Network'
  - a) Check if 'Adapter 1' is 'Attached to' a 'Bridged Adapter' with the Network Ethernet Card 'Name' enpMMMM (the M depends on the PC) and if 'Adapter2' are 'Attached to' Virtual Network Card created above and 'Name' vboxnet0

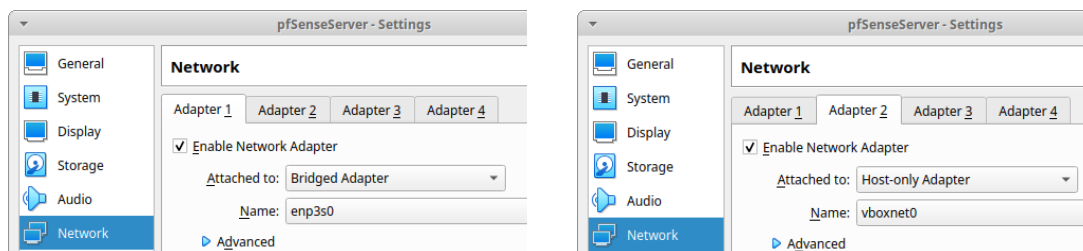


Figure 5: pfSenseServer Adaptors configuration (i)

- b) Go to 'Adapter3':
  - i. As with 'Adapter 1', it shall be of type 'Bridged Adapter';
  - ii. Go to the 'Name' drop down menu and select the Ethernet USB Adapter plugged in step 2; it shall be named 'enxMMMMMMMMMMMMMM', in line with what you saw in step 3.

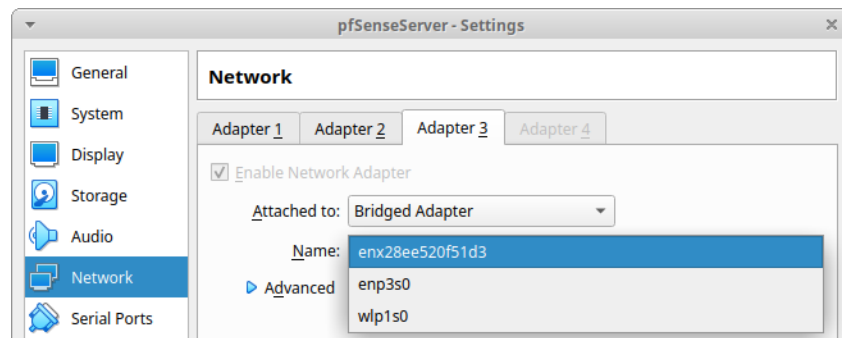


Figure 6: pfSenseServer Adaptors configuration (ii)

iii. Press 'OK'

9. Start the 'pfSenseServer' VM; when finished, you shall see the following screen.

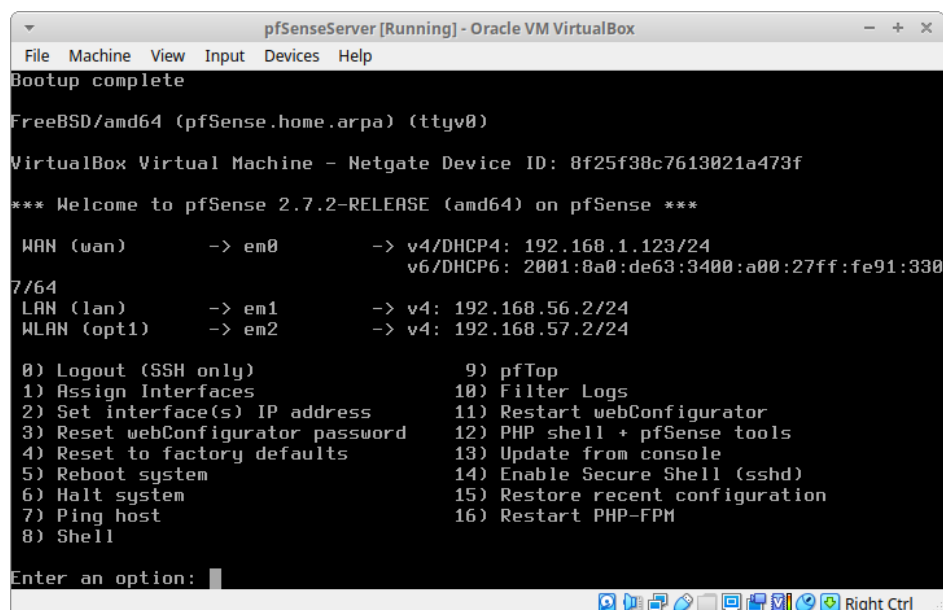


Figure 7: pfSense basic configuration menu

10. Register the different IPv4 addresses assigned to the WLAN, LAN and WLAN interfaces (come back to fig 1 at the beginning to better understand their meaning).

5. WLAN setup

11. Connect to the FiberGateway via WLAN:
- a) Use the SSID and credentials ('Rede/User'/Password') shown in Fiber Gateway bottom/base

b) Open a Browser, insert URL 'http://192.168.1.254' and use 'meo'/'meo' as login credentials
12. Go to 'Wi-Fi'
- a) In the 5GHz tab (see figure below):

i. Change 'Largura de banda' to 20 MHz

ii. Change WLAN 'Canal' (Channel) accordingly to the table below (if your device does not support that channel, try another one as close as possible)
- a) Press 'guardar'

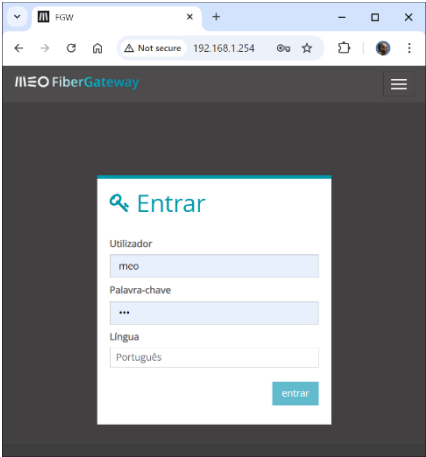


Figure 8: Fiber Gateway login screen

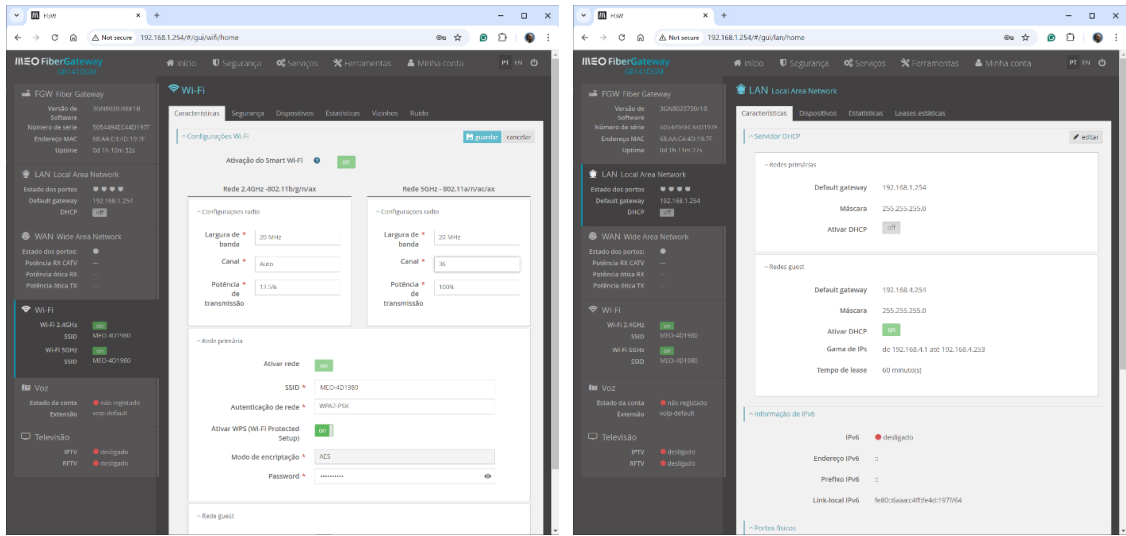


Figure 9: WLAN configurations

Group	Room/Channels	
	330	331
1	36	104
2	40	108
3	44	112
4	48	116
5	52	120
6	56	124
7	60	128
8	64	130
9	100	134

Table 2: WLAN channels to be configured

13. Go to 'LAN Local Area Network', 'Características', 'Servidor DHCP', 'Redes primárias' and press 'editar'
  - Turn to 'off' in 'Activar DHCP'; press 'guardar' (*pfSenseServer is the DHCP server also for the WLAN network*)

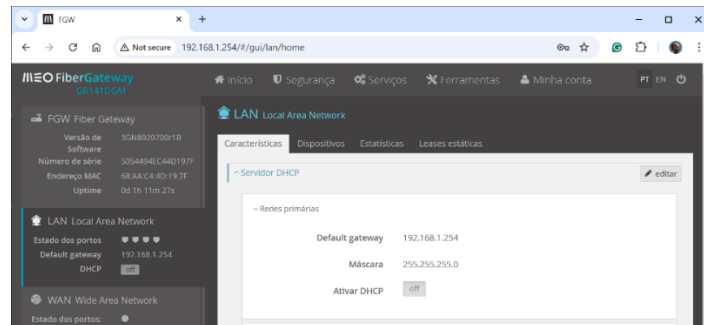
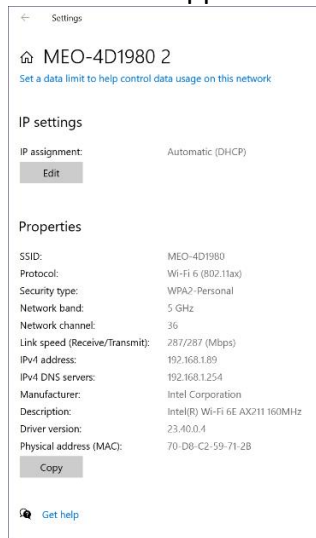


Figure 10: DHCP configuration

14. Only now connect the ethernet cable from the USB Adapter of your PC LAB to the Fiber Gateway, using one of the yellow Ethernet Ports in its back; pfSense DHCP server will configure terminals connected to the AP.
15. Disconnect your terminal from the AP and reconnect it to your Fiber Gateway SSID, in the Windows/Linux WLAN interface configuration; it will get a new IP configuration.

## 6. pfSense utilization

16. Verify in the WLAN network 'Properties', if it is connected to the right band and channel, with correct IP addresses (In iOS (and some other SO), the Captive Portal could appear immediately; if so, do not login yet)



*Figure 11: terminal configuration, when associated to the WLAN (example – you should get instead an IP from network 192.168.57.0/24)*

17. Check the assigned IP address, gateway and DNS servers of the WLAN interface (in a 'Terminal emulator', 'Command prompt' or similar console, issue command 'ip addr', 'ipconfig', or similar, depending in your OS).
18. Start a non-stopping ping to the laboratory ethernet network gateway (in Windows 'ping -t 192.168.100.1'); does it work? Leave it running even if it doesn't work (note: the -t option makes the ping work forever).
19. Open a browser and enter the URL [www.ua.pt](http://www.ua.pt); The captive portal to authenticate and allow Internet access shall appear
- if the Captive Portal takes some time to appear, open a second tab and enter URL [http://192.168.57.2:8002/index.php?zone=wlan\\_portal](http://192.168.57.2:8002/index.php?zone=wlan_portal)
20. Authenticate with the first listed, user1 ('cm'/'cm'; see Table 1)
- You shall succeed and get the UA Portal
21. See what happens to the ping
22. Start a speed test (use the associated test URL - <http://nperf.com>); register the obtained speed and interpret the values
23. Logout (if the 'Disconnect' button in the pfsense page is not visible, open a new tab and enter the same URL as above)
24. See what happens to the ping
25. Disconnect and reconnect with user2 ('cm\_band').
26. Go to the associated test URL (<http://nperf.com>), register the obtained speed and interpret the values
27. Disconnect and reconnect with user3 ('cm\_time'); start a "stopwatch" counter.



28. Observe the ping for more than 2 minutes, until it stops working and stop the “stopwatch”; register the obtained time and interpret the values. Is the user still connected?
29. Reconnect with user4 (cm\_traffic’).
30. Go to the associated test URL (<https://www.gns3.com/software/download-vm>) and start the downloading of a GNS3 image. Does it conclude? Interpret the results.

## 7. pfSenseConfig VM: VirtualBox installation and configuration

31. As with the pfSense VM, now, in the Desktop of the lab PC, double click the 'pfSenseConfig.ova' VM image and 'Import' it.
32. On its 'Settings' and 'Network', change 'Adapter 1' attachment to 'Host-only Adapter' and associated it to 'vboxnet0'; this will connect this VM to the 'pfSenseServer', through this internal network, with a DHCP server in pfSense (it shall be working by now and already configured for this).
33. Start the 'pfSenseConfig' VM and login to it ('labcom'/'labcom').
34. Open a 'Terminal emulator' and, with command 'ip address' check the assigned IPv4 address to the interface 'enp~~xxx~~'; it shall be in network 192.168.56.0/24.
35. Start a browser and enter the URL <http://192.168.56.2> you can use the link file in the desktop called pfSense Config)
36. Since pfSense server shall now be up and running, will get the following page:

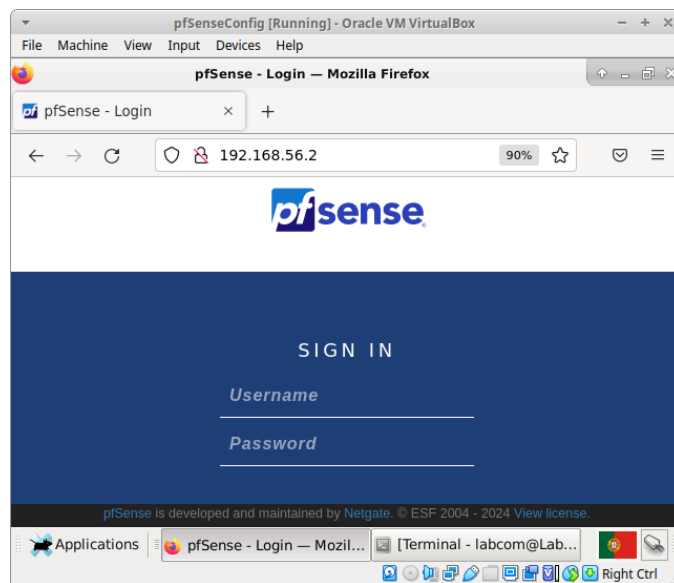


Figure 12: pfSense configuration portal

37. Login with credentials 'admin'/'pfSense'.
  - **DO NOT CHANGE ANYTHING UNLESS IT IS REQUESTED IN THIS GUIDE**
38. Go to 'Status' → 'Captive Portal'. Should not be any user logged in:

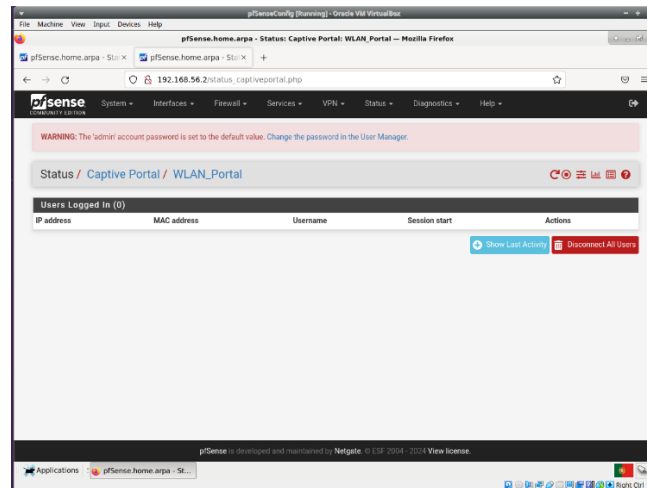


Figure 13: pfSense configuration portal

39. Connect other devices, like your Smartphones or Tablets, via WLAN to your Fiber Gateway SSID and start the authentication with different users
40. Repeat the steps before for User2 and User3 simultaneously and see what happened with the Logged Users.
41. Go to 'System' → 'General Setup' and observe the configured parameters.
42. Go to 'System' → 'Package Manager' and observe the existence of 'freeradius3'.
43. Go to 'System' → 'Routing' → 'Gateways' and observe the obtained (DHCP) configuration.
44. Go to 'Interfaces' → 'Assignments' and interpret the existing three correspondences.
  - Click in each of them and check their configuration.
45. Go to 'Firewall' → 'Aliases' → 'All' and interpret the list of shown IP addresses.
46. Go to 'Firewall' → 'Rules' → 'WLAN' and interpret the shown rule.
47. Go to 'Services' → 'DHCP Server' and interpret the LAN and WLAN configurations.
48. Go to 'Services' → 'DNS Forwarder' and interpret the configuration.
49. Go to 'Services' → 'Captive Portal' and edit the 'Zone' 'WLAN\_Portal'; interpret the configuration; pay attention to the defined 'Default download/upload' values.
50. Go to 'Services' → 'FreeRADIUS' and check the existence of the user 'labcom'; edit it and interpret the configured parameters; try to figure out what will happen to the sessions of this user.
51. Go into the editing mode of that user (the occulted password is 'labcom').
52. Go to the pfsenseServer VM and *halt the system* (option 6, 'Halt system').

- **DO NOT SHUTDOWN THE VM OR PC WITHOUT DOING THIS**

## 8. References

<https://www.youtube.com/watch?v=hqjE4KySvWU>

<https://docs.netgate.com/pfsense/en/latest/>

<https://www.pfsense.org/>