Workshop 7a – Firewalls

*Exercise 1 – Install **nginx** on your Ubuntu virtual machine.*

Ufw (*uncomplicated firewall*) is a command line interface to configure a firewall in Linux. This tool is already installed on your machine. Run:

- sudo ufw status verbose

Activate your firewall:

- sudo ufw enable

Also activate logging (in the */var/log/ufw.log* file):

- sudo ufw logging on

Try to log in to your Linux server **via ssh**. It should not work. Check in the /var/log/ufw.log file.

To allow *ssh* connections:

- sudo ufw allow ssh

To see the current rules of the firewall:

- sudo ufw status verbose

To open a port, we run either:

- sudo ufw allow *port-number*
- sudo ufw allow *service-name*.

To find the names of the services, do:

- cat /etc/services.

Exercise 2 - Configure your firewall to allow access to your Web server as well as to your openssh server from the PC.

Here are some examples of rules:

- sudo ufw allow from 172.30.0.7/16
- sudo ufw delete allow from 172.30.0.7/16
- sudo ufw deny 53
- sudo ufw deny in on eth0 from 15.15.15.51
- sudo ufw allow from 15.15.15.0/24 to any port 3306

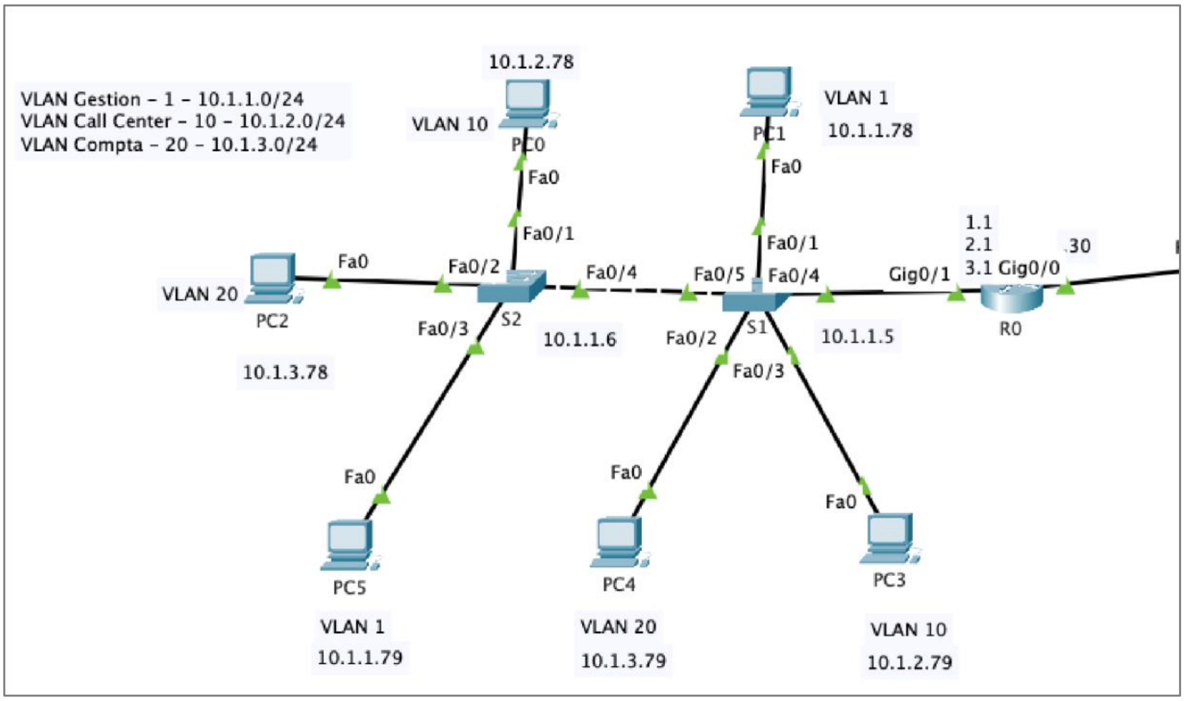
We can also see the rules with sudo ufw status numbered and then remove a rule with the command sudo ufw delete rule-number.

Important: the rules are evaluated in order: the first rule that can be applied is used.

Exercise 3 - Configure your firewall to allow access to the Web server from one colleague but prohibit access other colleagues.

Exercise 4 – configure your firewall for ssh, but with permission granted to different colleagues.

Exercise 5 – Network Access Control



Download the file CompanyNetwork.pkt from Cyber-Learn.

Add the following network security constraints:

1. Port security should be implemented on the ports for switches S1 and S2
2. Forbid **ssh** connections to the switches from VLAN 20
3. Forbid access from PC5 to the Web server at the address 188.76.65.16