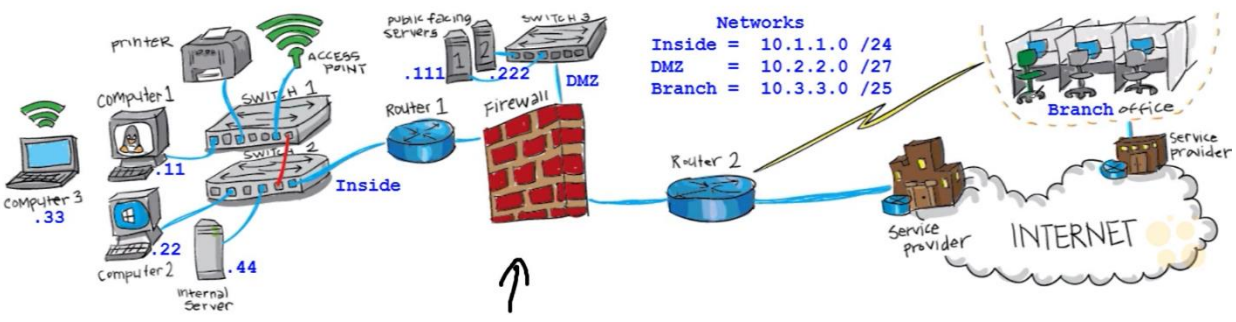
LAB2-Firewall (Pare-feu)

1. Install packet racer (Free version)
2. Design the same topology on cisco packet tracer but replace the hard ware Firewall Bridges by router to install a software firewall Router 3 of two interfaces one connected to the inside network passing through Router 1 IP@= 10.1.1. 66/24 and second interface is connected to the router 2 of IP@= 10.3.3.50/25.
   - **The Router 3 has three interfaces of IP addresses (int01: 10.1.2.66/24, int02: 10.3.4.50/25, int03: 10.2.2.1/27).**
   - **The Router 2 has three interfaces of IP addresses (int01: 10.3.3.57/25, int02: 10.3.4.58/25, int03: 10.3.5.59/25 (gateway toward the internet)).**
   - **The Router 1 has two interfaces of IP addresses (int01:** IP@= 10.1.1. 55/24 (connected to the inside network), **int02:** IP@= 10.1.2.77/24(**connected to the DMZ (firewall) router**)).
   - **The branch office is a group of 6 computers give each computer an IP address.**
     - Cmp1= 10.3.3.51/25,
     - Cmp2= 10.3.3.52/25,
     - Cmp3= 10.3.3.53/25
     - Cmp4= 10.3.3.54/25
     - Cmp5= 10.3.3.55/25
     - Cmp6= 10.3.3.56/25
   - **Replace internal server by 2 servers (** DNS server and FTP server**) of the following IP addresses:** IP@ DNS server= 10.1.1.44/24.
   - Server 1 is secured web server of HTTPs services having the IP @= 10.2.2.11/27.
   - Server 2 is a normal web server of HTTP services having the IP@= 10.2.2.22/27.



3. **Questions: (Take screen shoot for the firewall configuration, topology and all other configurations, save the cisco packet tracer file (.pkt) in your name and write a report with brief explanation.**
4. **The Network Admin of the network "Inside" want to Configure cisco firewall (enable access and deny filtering packet for the following statements):**
    a. **Authorize Computer 1 and computer 3 to have access to cmp2 and cmp3 consecutively.**
    b. **Allow the Web server HTTPS and Web HTTP accesses from computer 2.**
    c. **Deny the access of computer 2 to Web HTTP!!!**
    d. **As we see in (b) Computer 2 is authorized to accesses Web HTTP and (c) has denied the access!!**
        i. **If a user using Compter 2 try to request a web page google.com from Web server, will he have access to the page, if yes WHH? If no WHY?**
        ii. **The firewall read the Access Control List from top to bottom or from bottom to to?**
        iii. **What change should we do to interdict the access from Computer 2 to Web server.**
        iv. **After having a look on the ACL table we noticed that there is no confgured policies that allow or deny computer 1 to access the web server. In such a case if Computer 1 sent a request for a web page google.com could it reach the server or the request will fail? Justify?**
5. **The network Admin of the private network " Branch Office" want to Configure cisco firewall (enable access and deny filtering packet for the following statements):**
    a. **Allow any computer from internet to access any computer from Branch office.**
    b. **Allow any computer from Branch office to access any computer from inside network**
6. **Complete the ACL table below by hand for all the policies of part (4) and (5)**

Access Control List (ACL) case study

Permit or Deny	Protocol	Source IP	Source Port	Destination IP	Destination Port

Good Luck 😊