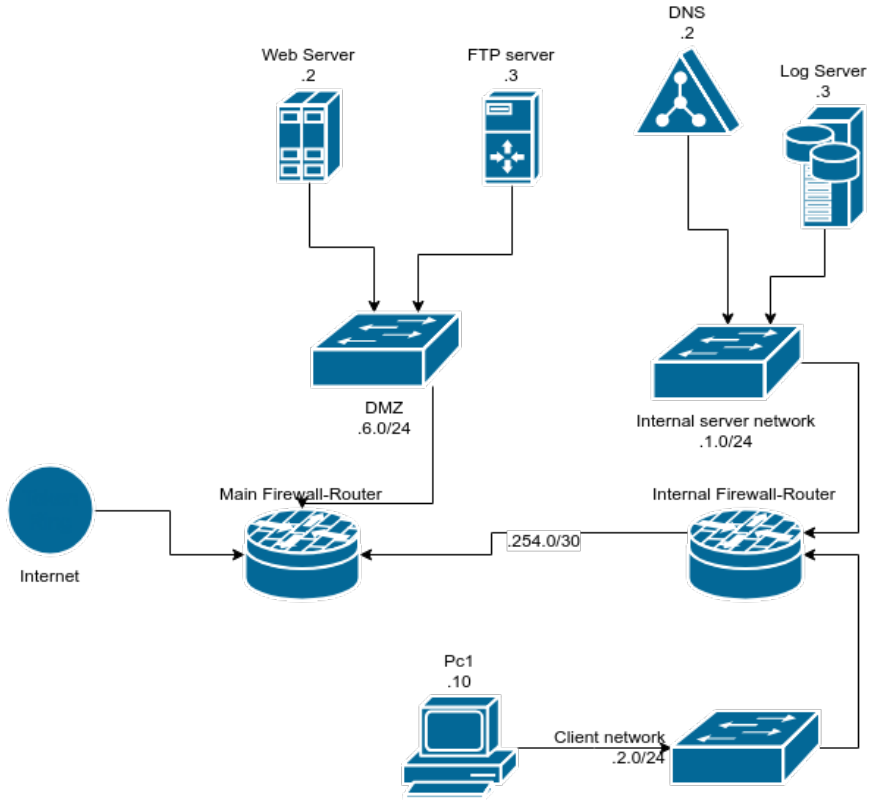
Assignment 3: iptables on ACME co. Single student activity

In this assignment you have to properly configure the network firewalls of the ACME co., according to the security policy, within the Kathará framework. The firewalls to be configure are the Main Firewall-Router (mainfw) and the Internal Firewall-Router (intfw). All the implementations have to be done with iptables. Please, include in the hand-in package also the scripts to properly reproduce your implementation. It is advisable to also prepare and include a testing script (or use the _test directory of Kathará) so that it is easy to check your configuration and ANY other implementation of the same policy.

You have to download the lab package and run the network. Here is the topology of the network of the ACME co.:



The Kathará lab.conf file for this assignment should be configure with all the required services, running. Pc1 in the Client network has the .10 IP address in the network.

Remember to add a route in the hosting machine so that you can reach the internal network and emulate a Internet, external host. The command could be something like this:

```
root@host # ip route add 100.64.0.0/16 via 172.56.0.2
```

where 172.56.0.2 should be set as the IP address assigned to eth0 interface of Main Firewall-Router (mainfw) when the lab is up and running (namely, after lstart command). Please note that the command requires administrative permissions (sudo or root user).

If there is something you suspect is wrong or is not as you expect, please write a comment in the Classroom page, so that all the students can see and, possibly, agree or disagree.

Security policy of ACME co.

- All the host have to use as DNS resolver the internal DNS.
- All the services provided by hosts in in the DMZ have to be accessible from the Internet.
- All the services provided by hosts in the Internal server network have to be accessible only by Client network and DMZ hosts.
- Anything that is not specifically allowed has to be denied.

- All the hosts (but the Client network hosts) have to use the syslog service on the Log server (syslog).
- All the host of the network have to be managed via ssh only from hosts within the Client network. There is the administrator user in every host, but the clients (admin:adminpass).

Services of the ACME co.

- A web service in the standard port (in web host of lab.conf)
- A ftp service in the standard port (demo:password), (in ftp host of lab.conf)
- A DNS in the standard port (in dns host of lab.conf)
- A syslog server in the UDP standard port (in syslog host of lab.conf)

Scheme of your hand-in

You have to prepare a document with the following structure:

Assignment 3: iptables on ACME co.

Student name:
Student matricola:

1. Introduction
2. Evaluation of the security policy
3. Policy implementation
4. Test of the configuration
5. Final remarks