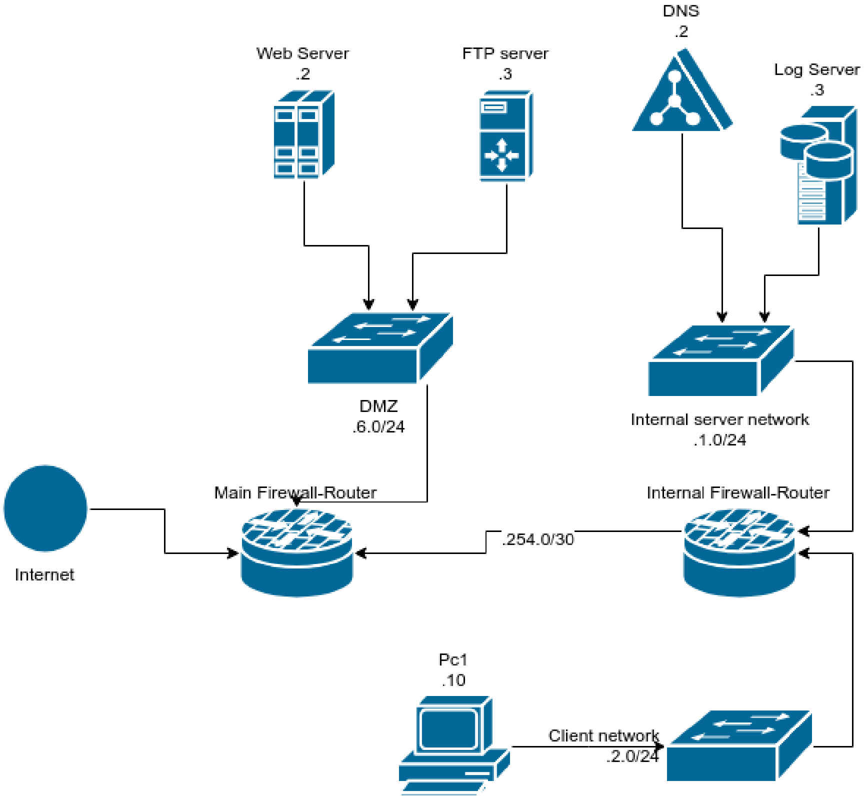
Assignment 4: opnsense on ACME co. Single student activity

In this assignment you have to properly configure the network firewalls of the ACME co., according to the security policy, within the Kathará framework and opnsense firewall. The firewalls to be configure are the Main Firewall-Router and the Internal Firewall-Router. All the implementations have to be done with virtual machines, within your preferred virtual manager (VMWare, Virtualbox or MacOs virt). This means that you have to create two Virtual Machines with the opnsense (https://docs.opnsense.org/) and connect them in order to reproduce the topology of the assignment.



Please, include in the hand-in package also the backup configurations of the two opnsense firewalls to properly reproduce your implementation. It is advisable to also prepare and include a testing script (or use the _test directory of Katharà) so that it is easy to check your configuration and ANY other implementation of the same policy.

NOTE: to discover the association between network and bridge interface and properly connect your VMs, you can use the network ls command of docker:

```
user@host $ docker network ls
NETWORK ID          NAME                DRIVER              SCOPE
bfd118ea9f66        bridge              bridge              local
4fc62cd87664        host                host                local
53ef51830a17        netkit_1001_DMZ     bridge              local
27d7ff69a9c5        netkit_1001_client  bridge              local
2b0014c1c20e        netkit_1001_server  bridge              local
813c61c87d84        none                null                local
```

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

Remember to setup the Main-Firewall-Router to use the hosting machine as the gateway so that you can reach the internal network and emulate a Internet, external host.

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).
- All the Client network hosts have to only access external web services (http/https).

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 4: opnsense on ACME co.

Student name:

Student matricola:

1. Introduction
2. Setup of the infrastructure

   Here you should detail the steps you've done to properly setup the two firewalls, how did you manage to connect the interfaces to both the host machine and the Katharà machines. You should also include details and explanation about the difficulties you've faced and solved.
3. Evaluation of the security policy
4. Policy implementation in opnsense
5. Test of the configuration
6. Final remarks