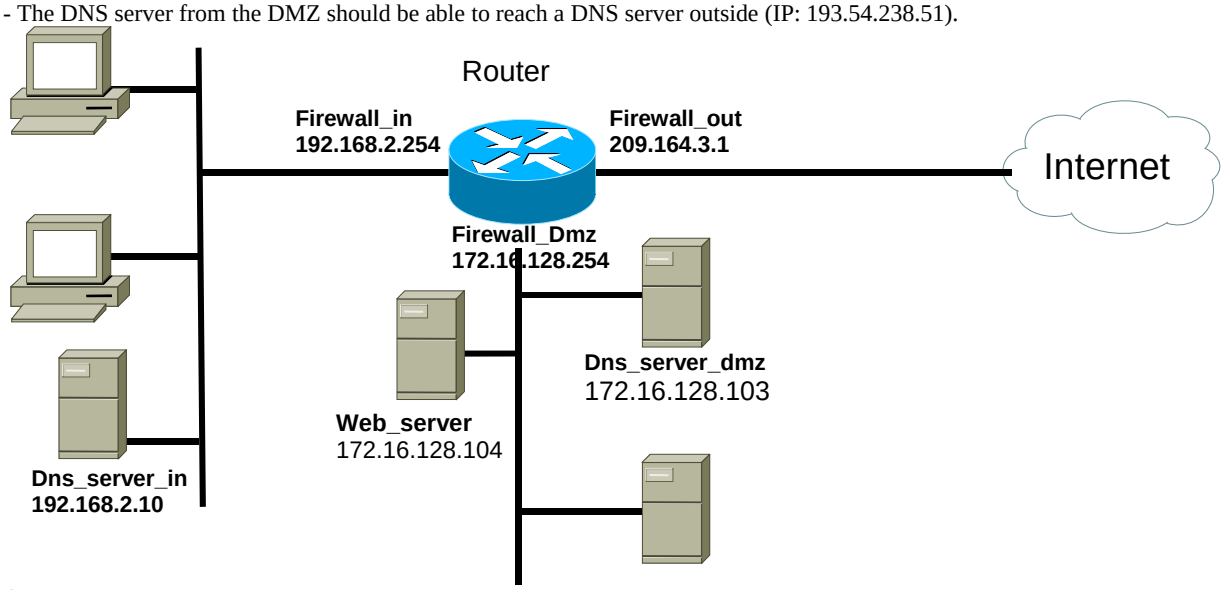
Exercise: Firewall

In order to ensure the security of a network, a firewall is used, at the interface between a "Network_in" (192.168.2.0/24) (corporate network), a "Network_Dmz" (demilitarized zone, 172.16.128.0/24), a "Network_out" (name of the network which is directly connected to the "out" (external) interface of the router, 209.164.3.0/24).

- Each machine from the inside network (Network_in) should be able to reach any machine outside (using a set of services "services_intra" composed of the following services: http, https, ftp).
- Each machine from the inside network should be able to ping a machine outside (icmp protocol).
- Each machine from the DMZ network (network_dmz) should be able to ping outside too.
- The DNS server from the inside network should be able to reach the DNS server of the DMZ (a set of services called "service_dns" is composed of tcp and udp protocols, on the port 53).
- The DNS server from the DMZ should be able to reach a DNS server outside (IP: 193.54.238.51).



Questions

1.1. Propose translation rules allowing the machines from the inside network to be connected on internet. Propose translation rules allowing the machines from the DMZ to be connected on internet.

We can use a syntax following the example below:

'Source port translated'

Source: IP address of the source machine or of the source network

Port: port (number (ex: 53) or protocol (ex: udp), it is possible to write 'none' or 'any', if necessary)

Translated: public IP address of the machine (or interface) achieving the translation.

Ex:

- 10.3.0.0 http 192.54.10.7
- 172.16.6.0 any 192.27.18.32

Ans:

Network_IN any 209.164.3.1

Network_DMZ any 209.164.3.1

1.2 Propose filtering rules allowing the machines from the inside network to be connected on internet to achieve *pings* and to be able to send requests to some *http, https* and *ftp* servers. Please give a comment about the filtering rules you use and justify them. Add some rules in order to ensure the correct functioning of the DNS servers.

We can use the following syntax:

'Protocol source destination service action'

Protocol: type of protocol (we can use 'any' if necessary)

Source: IP address of the source machine or of the source network (we can use 'any' if necessary)

Destination: IP address of the destination machine or of the destination network (we can use 'any' if necessary)

Service: port number (we can use 'any' if necessary). We can also here put a "set of services" (services_intra, services_dns…)

Action: 'pass' or 'block'

Ex:

- tcp 10.3.0.0 172.16.6.0 any pass
- icmp 10.3.0.4 any any block
- any 10.3.0.0 any services_intra pass

icmp Network_IN any any pass

icmp Network_DMZ any any pass

any Network_IN any services_intra pass

Note: services_intra regroups http, https and ftp services

any Dns_server_in Dns_server_Dmz services_dns pass

Note: services_dns regroups dns (tcp, udp) services

any Dns_server_Dmz 193.54.238.51 services_dns pass