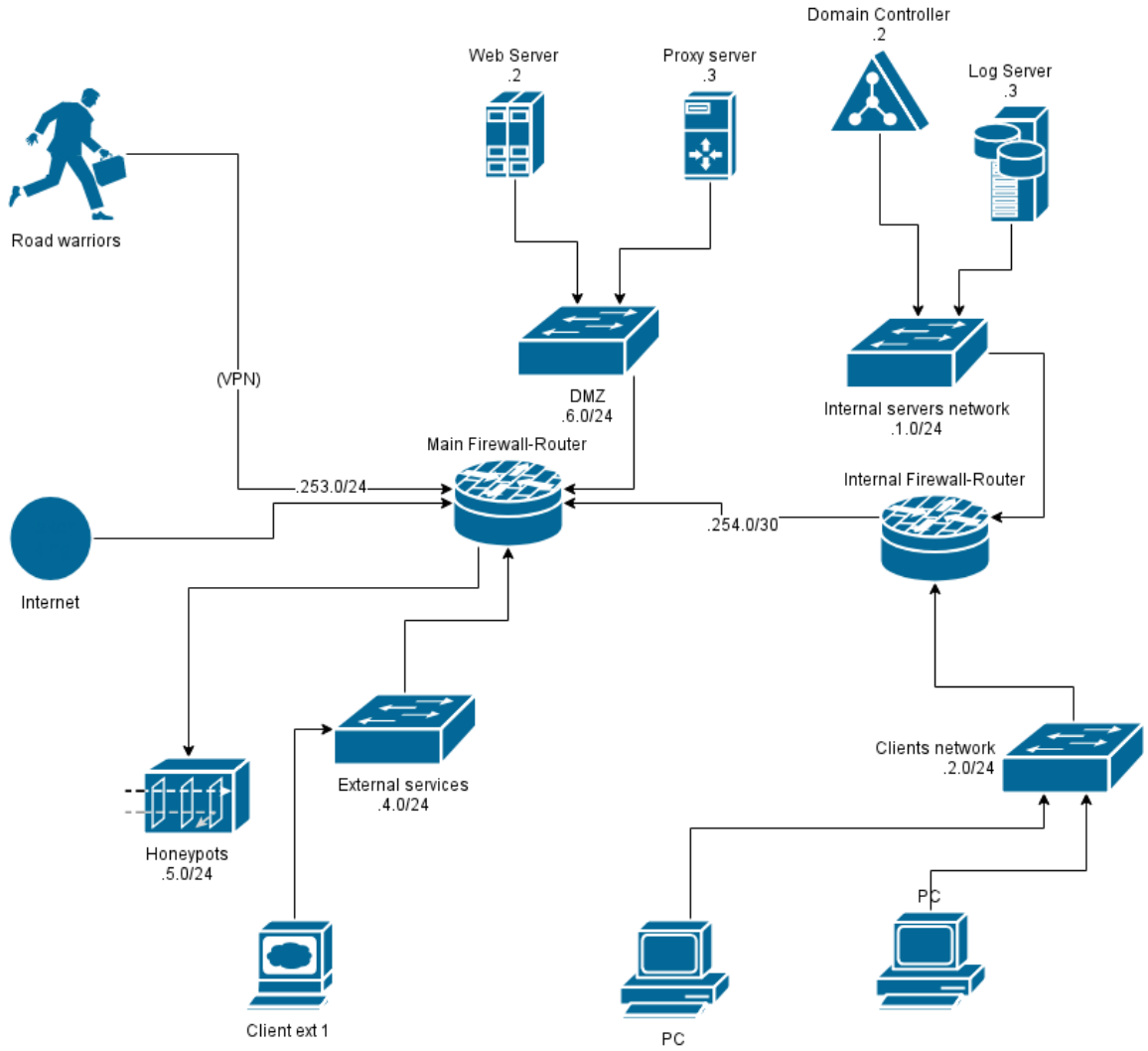
Assignment 7: suricata on ACME co. Group activity

In this assignment you have to properly configure the IPS suricata on both the network firewalls of the ACME co. You should do it within our remote infrastructure, but you can also use the infrastructure of Assignment 5.

You have to turn on the IPS from the GUI, update the rules and configure the IPS so that it can self-update the rule database.

Once the IPS is properly setup, you have to write two more rules to block the attacks your operators were able to capture in the two pcap files in attachment. The two attacks are of type UDP and TCP: you have to write a rule for both the protocols, so two rules. Moreover, you have to provide evidences that your rule actually works.



Scheme of your hand-in

You have to prepare a document with the following structure:

Assignment 7: suricata on ACME co.

Student names:
Student matricola list:

1. Introduction
2. IPS configuration
3. Custom rule writing and description
4. Test of the rules
5. Final remarks