My topology

A diagram of a network

Description automatically generated

Set the default gateway in suricata to be the ip of the router

A screen shot of a computer

Description automatically generated

Add in the router a static route to the network 10 that was not discovered

A computer screen shot of a computer program

Description automatically generated

Let suricata forward the packets to a certain queue



Start suricata



A screen shot of a computer program

Description automatically generated

Open the suricata.yaml file (main file containing the configuration)

A screenshot of a computer

Description automatically generated

Inspect the loaded rules

A black screen with white text

Description automatically generated

Comment suricata.rules and add myrules.rules instead.

A screenshot of a computer program

Description automatically generated

Run suricata

From h2 run a hh.py code

Inspect logs

A screen shot of a computer program

Description automatically generated

On fabric

<https://www.virtono.com/community/tutorial-how-to/how-to-install-suricata-on-ubuntu-22-04/>

<https://docs.suricata.io/en/suricata-7.0.2/install.html>

<https://github.com/OISF/suricata>

suricata rules were not found:

<https://docs.suricata.io/en/suricata-6.0.0/rule-management/suricata-update.html>

A screenshot of a computer

Description automatically generated

Edit interface suricata.yaml

A screenshot of a computer

Description automatically generated

Edit default rules directory:

A screen shot of a computer

Description automatically generated

Command to run : sudo suricata -vvvv -c /etc/suricata/suricata.yaml -i enp8s0np1