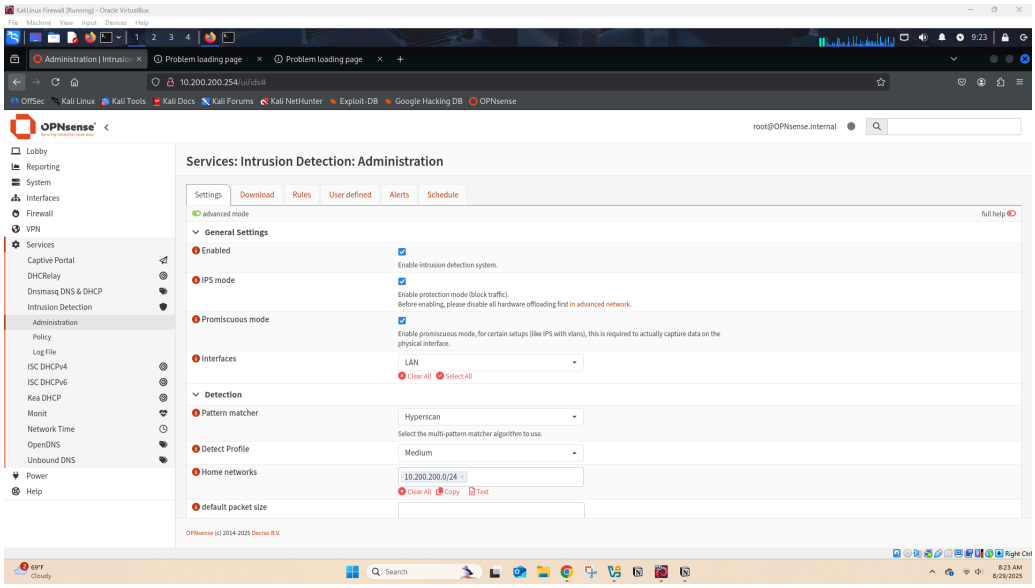
IPS & IDS Setup

Intrusion Prevention & Intrusion Detection features

Intrusion Detection System - A feature that we can install on our firewall/devices. That can detect for any malicious activity based on what we configure the IDS to look out for.

Intrusion Prevention Systems - same as IDS but we can block or deny traffic or patterns.

IPS **Setup**



The image above takes a look at my IPS settings

- Enable - making sure IPS is on
- IPS mode - enable the ability to block traffic

- Promiscuous Mode - Enables for specific set ups, required to capture data on the physical interface
- Interfaces - I am running it on my LAN
- Pattern matcher - Different algorithms to find intrusion patterns (Hyper scan is more modern)
- Detect Profile - set to medium so its not too aggressive causing false positives
- Home networks - this will be the ip address I created earlier in the installation
- Syslog alerts - I will enable this to send alert to the system log.
- Rotate log - how many logs need to be kept & how often do you want to rotate the logs. (weekly, 4).

OPNsense bases their IDS/IPS system on the Suricata, which allows us to write custom rules