Greetings Team!

With all the traffic that is streaming in and out of our network, we really need some way to filter it all to make sure things are clean. In addition, we also need some sort of system to let us know if our network got intruded upon.

Since it looks like we have a OpenSense router, please set it up with the integrated IPS (Suricata) platform within OpenSense. Create a report on how you were able to set it up as well. I feel this should really help create a dam against network attacks as well as help alert us when things do happen.

Once you set it up, provide an additional report on what rules you have set up on the system as well as any additional rules you may have added in addition for our particular company and types of traffic that it handles.

When it has been set up, let it run for a couple hours. This will assist you in gathering the necessary material for the second report coming in on another inject.

Isaac Waterfield  
CTO