Date:
Subject: Network Security OpenSense IPS Configuration

Hello [sender],

Thanks for your directive. We understand the importance for effective traffic filtering and intrusion detection. We plan to address this by setting up the Suricata, the integrated IPS, platform within the OpenSense router.

Hopefully this summary of the steps taken to configure the OpenSense router with Suricata will benefit you:

1. Access OpenSense Dashboard:
   Log in to the OpenSense dashboards.
2. Navigate to Suricata Settings:
   Locate and access the Suricata settings within the OpenSense interface.
3. Enable IPS:
   Activate the Suricata IPS module
4. Configure Rules:
   Set up default rule and customize them to align with our company's needs.
5. Additional Rule Configurations: (list here)
   Implement specific rules tailored to our company's traffic and security requirements.

This email provides a high-level overview of the Suricata setup and we are more than willing to provide a comprehensive explanation. We will begin working on a detailed report outlining the configuration steps and choices made during the setup and configuration process.

Once configured, the system will run for a couple of hours to collect relevant data. Once completed, a second report will be created that includes information on the rules that were used, the purpose of the rule and any additional rules that were configured specifically for the network.

We respect your understanding of the importance of strengthening the network security, and we will ensure you that the configuration made to the system provides support to the networks defenses against attacks and provides timely alerts.

If any other questions or requirements come to mind for the configuration, please feel free to let us know.

Thank you.

Best regards,

[name]
[position]
[contact info]