Suricata - Feature #4285

Add an optional "active flow timeout" for long lived flows

01/29/2021 08:53 PM - Jeff Weeks

Status: New
Priority: Normal
Assignee: Jeff Weeks
Category: 
Target version: 
Effort: 
Difficulty: 

Label: 

Description

YAF is a flow meter which has a feature whereby every 30 minutes a new record is created for a long lived flow. In order to implement a similar feature in Suricata, a new timeout can be added which, upon expiry, will close the current flow, and open a new one (thus also generating a new flow record).