Suricata - Feature #3306
Support AF_XDP capture method
11/02/2019 09:10 AM - Eric Leblond

Status: In Progress
Priority: Normal
Assignee: Eric Leblond
Category: 
Target version: TBD
Effort: medium
Difficulty: high

Description
A new capture method has been recently introduced in Linux. Named AF_XDP, it allows to capture the traffic with a kernel bypass. This limit the cost of the capture in term of CPU cycle.

Related issues:
Related to Task #3288: Suricon 2019 brainstorm
Related to Task #4097: Suricon 2020 brainstorm

History
#1 - 11/02/2019 09:15 AM - Eric Leblond
Beginning of implementation using libbpf: https://github.com/regit/suricata/tree/af-xdp-v2

#2 - 11/02/2019 09:17 AM - Eric Leblond
- Parent task set to #3288

#3 - 11/02/2019 10:12 AM - Victor Julien
- Status changed from New to Assigned
- Assignee set to Eric Leblond
- Target version set to TBD

Set target to TBD as we are waiting for the kernel to provide us with timestamp support.

#4 - 11/05/2019 10:50 AM - Victor Julien
- Parent task deleted (#3288)

#5 - 11/05/2019 10:50 AM - Victor Julien
- Related to Task #3288: Suricon 2019 brainstorm added

#6 - 11/10/2020 03:43 PM - Victor Julien
- Related to Task #4097: Suricon 2020 brainstorm added

#7 - 10/20/2021 10:07 AM - Victor Julien
- Status changed from Assigned to In Progress