Suricata - Feature #2628

Specify the flow direction in metadata sent by Suricata.

10/03/2018 05:36 PM - Daniel Jaraud

Status: Assigned
Priority: Normal
Assignee: Daniel Jaraud
Category:
Target version: TBD
Effort:
Difficulty:

Description
I'm using Suricata to create parallel coordinates graphs with Vega from the dest/source ips and ports. Due to bandwidth issue, I can't use flow/netflow but can only rely on the http/dns/smtp/tls etc... data sent by Suricata.
Currently, the metadata sent from Suricata uses src_ip and dest_ip for the home network to protect as well as for the answer from the distant network.
For instance, in case of a DNS request, the first request from the client will set src_ip with the correct IP address of the client of the home network.
But, for the answer from the DNS server to the client, src_ip will then be set to the DNS server IP.
When drawing parallel coordinates graphs, this will lead to a mirror/vertical symmetry axis because src_ip (left axis for instance) and dest_ip (right axis) will show the same data.
Apart from using flow_id as a unique identifier and just draw the first occurrence of it (=> I'll have only the initiating link), is there another possibility, such as adding a new field to the data (such as I : initialization, R : related to an existing flow_id)?

Related issues:
Related to Feature #2644: Add direction of stream to eve-json events

History
#1 - 05/23/2019 09:55 PM - Andreas Herz
- Assignee set to Community Ticket
- Target version set to TBD

#2 - 05/24/2019 05:37 AM - Daniel Jaraud
Hello,
This feature has already been written: https://github.com/OISF/suricata/pull/3521#issuecomment-446604186. I have written the test for suricata-verify and published a MR, which is currently waiting for merging.

#3 - 05/27/2019 08:54 PM - Andreas Herz
- Status changed from New to Assigned
- Assignee changed from Community Ticket to Daniel Jaraud

Thanks for the contribution and the update here!

#4 - 09/26/2019 01:35 PM - Victor Julien
- Related to Feature #2644: Add direction of stream to eve-json events added