Suricata - Feature #3531
app-layer: signal stream engine about expected data size with next character
03/16/2020 09:43 AM - Philippe Antoine

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

Description
Currently the TCP based app-layers assemble the buffer they work on themselves. This leads to unnecessary buffering and code complexity. Instead, the app-layer API should allow the parsers to signal to the stream layer below how much data they need before the record is complete.

This can be with a specified length, or with a new expected character, for instance in text protocols such as FTP where we wait for end of line.

Related issues:
Related to Feature #3444: app-layer: signal stream engine about expected data...

Closed

History
#1 - 03/16/2020 09:43 AM - Philippe Antoine
- Parent task set to #3444

#2 - 03/16/2020 10:01 AM - Victor Julien
Some thoughts:

- we should think about a limit. If the requested char does not appear in the stream, queuing should not be endless.
- is registering a single char enough or do we have a need for registering multiple at once?

#3 - 03/16/2020 10:07 AM - Philippe Antoine
Nice thoughts.

Limit is needed indeed.

A simple char may not be enough... As end of lines can get tricky (cf SSH split between CR and LF)
Maybe a callback function hasEnoughData will be more generic ?

#4 - 03/18/2020 06:34 AM - Victor Julien
- Parent task deleted (#3444)

#5 - 03/18/2020 06:34 AM - Victor Julien
- Related to Feature #3444: app-layer: signal stream engine about expected data size added

#6 - 03/18/2020 06:54 AM - Philippe Antoine
Maybe the app layer parser can just signal to the TCP engine : this is not complete, keep buffering...
And be responsible for the limit they use...