Suricata - Feature #2280

http: rules that match both request and response

11/20/2017 09:51 AM - Victor Julien

Status: Assigned
Priority: Normal
Assignee: Victor Julien
Category: TBD
Target version: TBD
Effort:
Difficulty:
Label:

Description
Introduce support for matching on fields from both request and response side in a single rule in http.

This will have some limitations around body matching.

Related issues:
- Related to Task #2309: SuriCon 2017 brainstorm
- Related to Task #3288: Suricon 2019 brainstorm

History
#1 - 11/30/2017 07:27 AM - Andreas Herz
- Assignee set to OISF Dev
- Target version set to TBD

#2 - 12/01/2017 05:01 AM - Victor Julien
- Status changed from New to Assigned
- Assignee changed from OISF Dev to Victor Julien

#3 - 12/01/2017 05:01 AM - Victor Julien
- Related to Task #2309: SuriCon 2017 brainstorm added

#4 - 11/05/2019 10:54 AM - Victor Julien
- Related to Task #3288: Suricon 2019 brainstorm added

#5 - 09/08/2021 02:34 PM - Philippe Antoine
I do not understand what is expected here...

#6 - 10/19/2021 02:59 AM - xiaolong li
Philippe Antoine wrote in #note-5:

I do not understand what is expected here...

How to match http GET request with 404 NOT FOUND response?