Suricata - Feature #843
Custom http logging filter functionality
07/01/2013 04:58 AM - Roberto Martelloni

<table>
<thead>
<tr>
<th>Status:</th>
<th>New</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee:</td>
<td>Community Ticket</td>
</tr>
<tr>
<td>Category:</td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td>TBD</td>
</tr>
<tr>
<td>Effort:</td>
<td></td>
</tr>
<tr>
<td>Difficulty:</td>
<td></td>
</tr>
<tr>
<td>Label:</td>
<td></td>
</tr>
</tbody>
</table>

Description
I think can be useful to have a blacklist filter functionality to disallow HTTP logging of web sites that match a list of regex on FQDNs.

From my point of view having logs about some web site like for example advertising web sites it's not useful from a security point of view and also it's a waste of hard disk space and computational power.

I thin can be useful to have an external file (ex: disable_http_logging.sites) that contains a list of regex (ex: *.google\.com, *.advertising\.com) that disallow HTTP logging functionality on matched regexp.

Related issues:
Related to Feature #1005: conditional logging: controlling what gets logged

History
#1 - 10/25/2013 10:21 AM - Victor Julien
- Target version set to TBD

#2 - 08/25/2016 06:32 AM - Victor Julien
- Assignee deleted (Victor Julien)

I think it could be interesting to make the logging depend on the rule language. E.g. by adding something like 'log:yes;' or 'log:no;'.

#3 - 09/08/2016 02:49 PM - Andreas Herz
- Assignee set to Anonymous

#4 - 07/17/2018 08:44 AM - Victor Julien
- Related to Feature #1005: conditional logging: controlling what gets logged added

#5 - 07/17/2018 08:45 AM - Victor Julien
Probably best implemented as suggested in #1005

#6 - 02/23/2019 10:12 PM - Andreas Herz
- Assignee set to Community Ticket