**Suricata - Feature #276**

**Libcap support for dropping privileges**

03/17/2011 02:57 AM - Victor Julien

<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>medium</td>
</tr>
<tr>
<td>Difficulty</td>
<td>low</td>
</tr>
</tbody>
</table>

**Description**

On Linux we use libcap-ng to drop privileges after startup. Currently libcap-ng supports Linux only, so we need a different solution for FreeBSD and Mac OS X.

Using libcap would likely work.

**Requirements:**
- A solution would have to be coded up into src/util-privs.c.
- As much as possible the API should remain the same.
- configure.in/autotools need to auto detect presence and usability of libcap
- libcap-ng (if present) needs to have preference over libcap

Alternatively, libcap-ng could be improved. The upstream dev has indicated to be willing to accept patches for other operating systems.

**Related issues:**

Related to Feature #2375: Design and implement sensible per-thread capabilities  
Related to Feature #2931: Perform privdrop without libcap-ng support

**History**

#1 - 07/04/2012 03:43 AM - Victor Julien
- Target version set to TBD

#2 - 12/19/2017 02:22 AM - Victor Julien
- Related to Feature #2375: Design and implement sensible per-thread capabilities added

#3 - 07/13/2018 08:17 PM - Victor Julien
- Effort set to medium
- Difficulty set to low

#4 - 03/11/2019 02:06 PM - Victor Julien
- Assignee set to Community Ticket

#5 - 04/11/2019 06:21 PM - Victor Julien
- Related to Feature #2931: Perform privdrop without libcap-ng support added