Suricata - Feature #1002

Possible to disabling/bypassing a rule by a specific source ip and a destination ip?

10/18/2013 03:41 AM - Hang Cheung

<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>
</tbody>
</table>

Description

Dear Support,

In IDS mode, we could suppress the alert by defining a "track by_src" / "track by_dst". Is it possible to do the same in IPS mode, disabling a particular rule, when a source ip / destination ip / both matched, without modifying the rule itself?

Regards,
Hang

History

#1 - 10/26/2013 10:21 AM - Victor Julien
- Target version set to TBD

#2 - 09/18/2014 05:36 AM - Andreas Herz
This is also related to the general suppress behaviour: https://redmine.openinfosecfoundation.org/issues/1247

#3 - 12/22/2015 05:40 PM - Andreas Herz
- Assignee set to Andreas Herz

#4 - 06/16/2016 03:07 AM - Victor Julien
- Tracker changed from Support to Feature
- Assignee changed from Andreas Herz to Anonymous

Not sure how this should look in a rule:

suppress gen_id 1, sig_id 12345, track by_both, ip 1.2.3.4, ip 5.6.7.8
suppress gen_id 1, sig_id 12345, track by_src, ip 1.2.3.4, track by_dst, ip 5.6.7.8

Not very pretty.

Maybe track by_flowbit would be a better solution, then you can have a regular rule to set the bit. Of course you can also use flowbits directly in the rule you wish to suppress, but this may be simpler when adding exceptions to an existing ruleset.

#5 - 02/23/2019 10:13 PM - Andreas Herz
- Assignee set to Community Ticket