Suricata - Documentation #3222

Configuring ipv6

10/05/2019 08:40 PM - Daniel Vein

<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>Affected Versions:</td>
<td>4.1.2</td>
</tr>
<tr>
<td>Difficulty:</td>
<td></td>
</tr>
<tr>
<td>Label:</td>
<td></td>
</tr>
</tbody>
</table>

Description

suricata.yaml documentation doesn't mention how to set up ipv6 for HOME_NET var or host-os-policy.

For HOME var it shows multiple ipv4 like so: HOME_NET: "[192.168.0.0/16,10.0.0.0/8,172.16.0.0/12]"
As you can see there are no spaces between commas. But if you have HOME_NET: "[192.168.0.0/16,2001:1234:5678:1234::/64]"
suricata will fail to start without giving any ERRCODE.
To get it run you need a space after the comma for the ipv4 net like HOME_NET: "[192.168.0.0/16, 2001:1234:5678:1234::/64]"

For host-os-policy: you need to quote the ipv6 net like so

linux: [192.168.0.0/16, "2001:1234:5678:1234::/64"]

I think this should be better documented.

History

#1 - 10/07/2019 08:46 PM - Andreas Herz
- Assignee set to Community Ticket
- Target version set to TBD

Would you like to contribute the updated documentation?

#2 - 10/14/2019 11:11 PM - Daniel Vein
I'd love to help any way I can

#3 - 10/20/2019 08:43 PM - Andreas Herz
That's great, you can read how the best way to contribute should look like here:
https://redmine.openinfosecfoundation.org/projects/suricata/wiki/Contributing