Suricata - Bug #3638
TOS IP Keyword not triggering an alert
04/14/2020 01:06 PM - Brian Carlin

<table>
<thead>
<tr>
<th>Status:</th>
<th>Closed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee:</td>
<td>Jeff Lucovsky</td>
</tr>
<tr>
<td>Target version:</td>
<td>6.0.0rc1</td>
</tr>
<tr>
<td>Affected Versions:</td>
<td>5.0.2</td>
</tr>
</tbody>
</table>

Description
TOS flag does not trigger an alert for DSCP tagged packets when processing pcap. In the pcap below, there are packets tagged with AF41 (34) and EF (46).

[https://drive.google.com/file/d/1XpWTWNeIRCKEeXG7Wa3e1Gjkc0a4lU4wi/view?usp=drive_open](https://drive.google.com/file/d/1XpWTWNeIRCKEeXG7Wa3e1Gjkc0a4lU4wi/view?usp=drive_open)

I can filter this traffic in wireshark:
ip.dsfield.dscp  34 or ip.dsfield.dscp  46

I have tried several rule permutations (see below) to try and get an alert to fire. Can anyone point me in the right direction?

alert ip any any -> any any (msg:“Differentiated Services Codepoint: AF41”; tos:34; flow:to_server; classtype:not-suspicious; sid:202004; rev:1;)

alert ip any any -> any any (msg:“Differentiated Services Codepoint: AF41”; tos:34; classtype:not-suspicious; sid:202004; rev:1;)

alert ip any any -> any any (msg:“Differentiated Services Codepoint: AF41”; tos:34; flow:established; classtype:not-suspicious; sid:202004; rev:1;)

History
#1 - 04/26/2020 11:17 AM - Victor Julien
- Status changed from New to Assigned
- Assignee set to Jeff Lucovsky
- Target version set to 6.0.0rc1

#2 - 05/02/2020 02:12 PM - Jeff Lucovsky
- Status changed from Assigned to In Review

[https://github.com/OISF/suricata/pull/4914](https://github.com/OISF/suricata/pull/4914)

#3 - 06/09/2020 12:27 PM - Jeff Lucovsky
- Status changed from In Review to Closed