**Suricata - Bug #3834**

**Suricata 'content' keyword does not match on IP *payload* when using IP keywords**

07/19/2020 10:59 AM - Maayan Fish

<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></td>
</tr>
<tr>
<td>Category:</td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td></td>
</tr>
<tr>
<td>Affected Versions:</td>
<td>5.0.2</td>
</tr>
<tr>
<td>Difficulty:</td>
<td></td>
</tr>
<tr>
<td>Label:</td>
<td></td>
</tr>
</tbody>
</table>

**Description**

I tried matching an IP packet *payload* using the 'content' keyword, with no success. It only happened when I used IP keywords within the rule ('fragbits', 'fragoffset', 'ip_proto').

I'm using an IP packet that has type of "ip_proto"=4, which is IPinIP. Basically IPinIP is used for tunnels/VPNs and there are 2 IP headers one after the other. The first IP is usually to the target VPN server, and the second is to the internal host in the VPN's LAN. Only after those two IP headers comes the TCP/UDP/ICMP/etc payloads.

The first IP header starts at offset 0xE - "45 00", and the second IP header starts at offset 0x22 - "4f 00"

```
0000 f4 a9 97 d4 4e 62 08 00 27 8f 8a 93 08 00 45 00 ....Nb.....E.
0010 00 2c ab cd 20 00 40 04 2b 6e c0 a8 01 75 c0 a8 ....+n...u..
0020 00 cd 4f 00 00 64 00 01 00 00 40 00 72 97 7f 00 ..O...r...
0030 00 01 7f 00 00 01 00 00 00 00 ........
```

This is the rule I wrote trying to match the second IP header, which should be the content payload of the fist IP header. The second IP headers starts with "4f 00". This rule did not raise an alert.

```
alert ip any any -> any any (msg:"IPinIP content"; priority:1; fragbits: M; fragoffset: 0; ip_proto:4; content:"[4f 00]"; sid:11005081;)
```

However, when I removed the 'content' keyword, it did alert. In my view, the second IP header is the payload of the first IP header, and therefore 'content' keyword should match on it.

Is this a bug? Thanks