Suricata - Feature #1995

fast.log should show if packet has been dropped or rejected

12/21/2016 04:18 AM - Jan Eagleman

<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

When managing a few thousand rules with a mixed drop/reject policy it might be useful for fast.log to show if a packet has been dropped or rejected, at the moment it can only show drop.

for example:

```
reject http $HOME_NET any -> $EXTERNAL_NET any (msg:"ET POLICY HTTP Request to .su TLD (Soviet Union) Often Malware Related"; flow:established,to_server; content:".su\0d 0a"; http_header; pcre:/Host\x3A\x20\[^

 classify:trojan-activity; sid:2014170; rev:2)
```

Shows this in fast.log

```
12/21/2016-17:23:33.897239 [Drop] [**] [1:2014170:2] ET POLICY HTTP Request to .su TLD (Soviet Union) Often Malware Related [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 192.168.2.12:12507 -> 104.25.73.38:80
```

History

#1 - 12/21/2016 07:58 AM - Jason Ish

Looks like Snort does this as well with possible values being:
- Allow
- CDrop
- WDrop
- Drop
- FDrop

so breaking compatibility with Snort should not be an issue, would just want to verify some Snort output.

Reason: I think fast.log is one of the things we should stick with Snort compatibility if we can, as that is where the format is from and existing tools may be depending on it.

#2 - 01/04/2017 03:04 PM - Andreas Herz

I had a similiar request some time ago, wanted the "WDrop" but after some thinking I would prefer better wording. Maybe as an option to choose between snort compatible and some other?

#3 - 02/10/2017 02:15 AM - Victor Julien

- Status changed from New to Assigned
- Assignee set to Jason Ish
- Priority changed from Normal to Low
- Target version set to 70

#4 - 03/12/2019 11:01 AM - Victor Julien

- Status changed from Assigned to New
- Assignee changed from Jason Ish to Community Ticket
- Priority changed from Low to Normal
- Target version changed from 70 to TBD