

## pfSense Packages - Bug #9403

### Suricata - Checkbox 'Traffic Flows' enables logging for both logging formats

03/16/2019 03:43 PM - Julian Wecke

<b>Status:</b>	New	<b>Start date:</b>	03/16/2019
<b>Priority:</b>	Normal	<b>Due date:</b>	
<b>Assignee:</b>		<b>% Done:</b>	0%
<b>Category:</b>	Suricata	<b>Estimated time:</b>	0.00 hour
<b>Target version:</b>		<b>Affected Architecture:</b>	
<b>Affected Version:</b>			
<b>Description</b>			
<p>The checkbox 'Traffic Flows' in 'EVE Output Settings' now enables netflow and flow output. (net)flow logging is quite heavy. Usually you log either flow or netflow but not both simultaneously. The webgui should give an option to choose the format. Easiest way would be a 2nd checkbox. Such would still allow to log in both formats when somebody has a need for it.</p>			

#### History

##### #1 - 03/21/2019 08:40 PM - Bill Meeks

This is fixed in the latest 4.1.3 version of the Suricata package that is currently posted for review and merge into the pfSense 2.5 DEVELOPMENT tree. Here is the pull request: <https://github.com/pfsense/FreeBSD-ports/pull/631> was merged on March 22, 2019.

This issue can be closed.