pfSense Packages - Feature #6866

Suricata multiple interfaces

10/19/2016 04:30 PM - Idar Lund

Status:	New	**Start date:**	10/19/2016
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Suricata	**Estimated time:**	0.00 hour
Target version:			

Description

I've set up Suricata on the WAN interface. When an alert happen I don't see what internal address caused the alert. It is not possible to configure Suricata to show the internal (NAT) affected IP instead of the wan IP, because the Suricata process will only see the the traffic as it comes from or is sent to the WAN interface.

The workaround I did was to set up Suricata on the internal interfaces instead, but the problem is that when having many vlans, we have to set up several Suricata processes (one for each interface).

The Suricata config does support several interfaces per process. It would be nice to have this configuration possibility in the pfsense GUI.