Hi,

a debian users has opened a bug [0] requesting some features, specifically he request support for an environment where interfaces may change from execution to execution.

The original text:

==== 8< ====
On my netbook I regularly change the interface, which is connected to the internet.
So maybe some day I need eth0, the next day wlan0 and also ppp0 (via UMTS) is often in use.

I want suricata check all the interfaces. All shall have the same ruleset. How can I tell suricata to do so, if possible at all?
One solution may be, to create and start suricata with a seperate configuration for eth0, one for wlan0 and one for ppp0.
But that is annoying. In snort it was possible, just to tell which interfaces shall be included, it was very easy.
Hope there is a same easy way in suricata.

==== 8< ====

[0] https://bugs.debian.org/861822

History

#1 - 05/24/2017 02:41 PM - Andreas Herz
- Tracker changed from Bug to Feature
- Assignee set to OISF Dev
- Target version set to TBD

#2 - 05/25/2017 03:24 AM - Victor Julien

Wonder if you could use `-i any`. Or maybe define all the interfaces in use in the yaml.