Suricata - Feature #3290
use config vars everywhere
10/31/2019 09:42 PM - Victor Julien

Status: New
Priority: Low
Assignee: OISF Dev
Category:
Target version: TBD
Effort:
Difficulty:
Label:

Description
The address and port vars are currently limited to specific uses. E.g. port vars can be in rules and in the vxlan config.

Maybe it would make sense to take a much simpler approach. Treat the vars more like macros in C, where the cpp simply replaces the macros with their value before the compiler compiles it.

History
#1 - 11/01/2019 08:16 AM - Jason Ish
Victor Julien wrote:

Maybe it would make sense to take a much simpler approach. Treat the vars more like macros in C, where the cpp simply replaces the macros with their value before the compiler compiles it.

I 100% agree. So just a simpler vars section maybe?

vars:

FILE_DATA_PORTS: "[$HTTP_PORTS,110,143]"

(of course keeping support for the "groups" we already have).

#2 - 11/05/2019 11:20 AM - Victor Julien
- Assignee set to OISF Dev
- Target version set to 6.0.0beta1

Yeah I think this makes sense.

#3 - 04/13/2020 03:17 PM - Jason Ish
- Priority changed from Normal to Low

#4 - 05/25/2020 03:28 PM - Victor Julien
- Target version changed from 6.0.0beta1 to 7.0rc1

#5 - 10/12/2020 10:10 AM - Victor Julien
- Target version changed from 7.0rc1 to TBD