pfSense Packages - Feature #6866

Suricata multiple interfaces

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

Status:	Rejected	**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.

History

#1 - 09/25/2019 02:24 PM - Bill Meeks

No, it is not possible to have Suricata see internal (post-NAT) addresses when it runs on the WAN. Suricata hooks into the network path in front of the packet filter firewall. Suricata always sees the IP addresses as they appear to the NIC hardware itself. So on the WAN, Suricata is seeing the packets before the firewall has "undone" the NAT.

This issue can be closed as REJECTED.

Bill

#2 - 09/25/2019 02:30 PM - Jim Pingle

- Status changed from New to Rejected

#3 - 09/26/2019 12:41 AM - Idar Lund

You are only covering the first half of the description - which is of no relevance except giving you some background information.
My proposal is to add support for adding several interfaces for one suricata process. And this is possible in the suricata config file itself.

#4 - 09/26/2019 06:56 AM - Bill Meeks

Idar Lund wrote:

> You are only covering the first half of the description - which is of no relevance except giving you some background information.
> My proposal is to add support for adding several interfaces for one suricata process. And this is possible in the suricata config file itself.

You are correct. Sorry that I misread your initial issue report. However, even though Suricata itself supports monitoring multiple interfaces with a single instance; the current GUI code would need a lot of changes in order to support that. I'm not convinced yet why it would be worth all the work. Not to mention that you then lose the ability to selectively stop or restart Suricata on a given interface. If you needed to update something on an interface, you would need to restart them all. Another limitation of that operating mode is that all the monitored interfaces would need to run the exact the same ruleset.

If you run using Legacy Blocking Mode or in just plain IDS mode (no blocking), the interface is operated in PCAP mode and placed in promiscuous

mode. So in the case of an interface with many VLANs defined, just monitor the parent interface only. Because of the promiscuous mode operation, all of the traffic of the VLANs running under that parent interface would be captured and analyzed.

Do you have a different use case in mind that I am missing? Currently, when weighing the work required to implement this feature against the benefits it affords, I'm not seeing the scales tip over to the "benefit side" yet.