pfSense Packages - Bug #7223

IPv4 Rules not working in Inline Mode

02/07/2017 07:00 AM - James Webb

Status:	New	**Start date:**	02/07/2017
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Suricata	**Estimated time:**	0.00 hour
Target version:			
Affected Version:	2.4	**Affected Architecture:**	

Description

After adding the following rule to custom.rules:

drop ip [108.74.97.21, 82.132.247.191] any <> $HOME_NET any (msg:"Suspicious Botnet Blocked";)

Expected behaviour:
Block any traffic flowing from listed IPs - Regardless of Inline or Legacy mode

Actual behaviour:
Blocks traffic and adds message to alerts in Legacy mode. In Inline mode nothing happens and traffic is allowed through.

Other observations:
On further inspection it would seem that since the pfSense 2.4.0 update no IPv4 rules are being blocked in Inline mode at all. Note that the addresses tested are IPv4 and that this observation regarding lack of IPv4 blocking may be part or all of the issue.

James

History

#1 - 02/07/2017 07:37 AM - Kill Bill

Just to be clear here - If you are looking at the Blocks tab, that is NOT the place to look at with the inline mode.

#2 - 02/07/2017 07:47 AM - James Webb

Kill Bill wrote:

> Just to be clear here - If you are looking at the Blocks tab, that is NOT the place to look at with the inline mode.

No we look in the Alerts tab for items highlighted in red. However, no red or black IPv4 alerts are showing because all IPv4 traffic is being allowed through as proven when we tested our rule on our own IP. In Legacy mode traffic from a flagged IPv4 address is blocked and in Inline mode it is allowed through.

James

#3 - 02/07/2017 07:52 AM - Kill Bill

Your own IP as in something from HOME_NET? Not exactly useful test either. In general, taking similar things to the forum before you have a clear bug somewhere is would be suggested.

#4 - 02/07/2017 07:56 AM - James Webb

Kill Bill wrote:

> Your own IP as in something from HOME_NET? Not exactly useful test either. In general, taking similar things to the forum before you have a clear bug somewhere is would be suggested.

No a public facing IPv4 address. Not from HOME_NET. This is a clear bug as IPv6 addresses are being filtered in Inline mode. IPv4 addresses were also filtered until we started testing on the pfSense 2.4 beta. No Suricata configs have changed.

#5 - 02/07/2017 01:56 PM - James Webb

James Webb wrote:

> Kill Bill wrote:
>
> > Your own IP as in something from HOME_NET? Not exactly useful test either. In general, taking similar things to the forum before you have a clear bug somewhere is would be suggested.
>
> No a public facing IPv4 address. Not from HOME_NET. This is a clear bug as IPv6 addresses are being filtered in Inline mode. IPv4 addresses were also filtered until we started testing on the pfSense 2.4 beta. No Suricata configs have changed.

#6 - 02/07/2017 03:57 PM - Joe Cordon

James Webb wrote:

> James Webb wrote:
>
> > Kill Bill wrote:
> >
> > > Your own IP as in something from HOME_NET? Not exactly useful test either. In general, taking similar things to the forum before you have a clear bug somewhere is would be suggested.
> >
> > No a public facing IPv4 address. Not from HOME_NET. This is a clear bug as IPv6 addresses are being filtered in Inline mode. IPv4 addresses were also filtered until we started testing on the pfSense 2.4 beta. No Suricata configs have changed.

Looks like you accidentally quoted a message without putting anything in the body there!

Just made an account to add that I've also experienced the same problem recently with my hardware, but decided to refrain from making a bug report as I assumed it was my inexperience mis-setting up the system, and not to mention but the pf-sense release was still beta. However, given the confusion above I've decided to make an account to document my experiences. I started with all default configs as far as I'm aware on the latest 2.4 BETA.
Upon adding a similar rule:

drop ip 79.140.192.0 any -> $HOME_NET any (msg:"BLOCKED Test Connection";)

I have found the same behaviour as James. Just to be clear, the address blocked is from a VPN that is completely independent of all local addresses encompassed in $HOME_NET.

I'm finding that on **legacy mode** I have Suricata working as expecting, blocking test connections from the VPN. In addition to this singular test address, other random botnets/probing connections (both IPv4 and v6) are dropped, as configured in the default rules.

However when switching to **inline mode**, I also experience that the above testing address is not blocked at all and connection attempts from it are allowed. In addition, regular IPv6 addresses are also blocked just like in legacy mode, however - be it coincidence or not - no IPv4 blocks are being shown on the log. It seems unlikely to me that this is because no rogue IPv4 connections are made to the server, as they were detected fairly frequently in Legacy mode. Thus, I suspect that these are not being picked up.

I imagine, as James mentioned, that the problem may revolve around this (being no IPv4 traffic being blocked), or as issue in default configurations. However as I said, I have little experience with Suricata, the little I have is only from testing it in the recent past. Therefore the problem may be more subtle, or James and I have fallen into the same trap whilst configuration so I am merely speculating.

#7 - 02/07/2017 04:15 PM - James Webb

That's very interesting to know that we are having similar issues Joe!

I hope that either this can be resolved or we can work together to find out what exactly is going on here.
I've updated to the latest builds tonight and still the issue persists. I thought I had fixed it by tweaking some settings, but it was in fact blocks from legacy mode still being present in the firewall ruleset prior to switching back to inline mode.

James

#8 - 02/28/2017 11:57 AM - Jim Thompson

- Priority changed from High to Normal

#9 - 06/07/2018 11:08 AM - Steve Yates

Hi all, is this still an issue with the spring 2018 updates to Suricata? There was a forum discussion about it that I seem to have misplaced but overall my understanding is the default detection of networks over-detected, and essentially whitelisted traffic to/from the router, which is of course everything.