pfSense - Bug #8408

invalid rule written due to ipv6 ipalias being present

03/31/2018 01:16 PM - Pi Ba

Status:	Resolved	Start date:	03/31/2018
Priority:	Normal	Due date:	
Assignee:	Jim Pingle	% Done:	100%
Category:	Rules / NAT	Estimated time:	0.00 hour
Target version:	2.4.3-p1		
Affected Version:	2.4.3	Affected Architecture:	All

Description

The following rule is generated due to a IPv6 alias being present, this is supposed to fill a array of vips6 , but adds a mode item for the vips array. This causes the empty rule..

```
pass out  route-to ( em0 192.168.0.1 ) from  to !/ tracker 1000017468 keep state allow-opts label
"let out anything from firewall host itself"
```

Fix: https://github.com/pfsense/pfsense/pull/3924

History

#1 - 04/05/2018 02:33 PM - Jim Pingle

- Assignee set to Jim Pingle

I was finally able to replicate this and confirm the fix, PR merged, thanks!

#2 - 04/05/2018 02:33 PM - Jim Pingle

- Status changed from New to Feedback

#3 - 04/09/2018 11:25 AM - Jim Pingle

- Status changed from Feedback to Resolved

Problematic test cluster has no errors on a snapshot containing the fix. Looks good here.

#4 - 05/03/2018 01:21 PM - Jim Pingle

- Target version changed from 2.4.4 to 2.4.3-p1

#5 - 05/16/2018 02:55 AM - Rudolf Mayerhofer

I've started seeing this behaviour after upgrading the slave node of my cluster setup to 2.4.3_1
Thankfully the primary node is still on 2.4.3 and working just fine

Unfortunately this is likely not fully fixed!

#6 - 05/16/2018 03:04 AM - Eric Machabert

After upgrade from 2.4.2_P1 to 2.4.3_P1, having a cluster configuration with a WAN interface holding an IPV4 CARP AND an IPV6 CARP the problem is back.

It looks like the code parsing the VIPs in filter.inc misunderstand the IPv6 CARP VIP as a ipV4 VIP so it enter the ipv4 loop and because " $gw = get_interface_gateway($ifdescr)" returns the IPV4 GW, then tries to generate the pass out rule on empty values...

I removed my IPV6 CARP on the WAN interface and there is no more problem.

#7 - 05/16/2018 11:41 AM - Jim Pingle

Anyone else hitting what they believe is this bug is probably hitting [#8518](#) instead. Put comments there.