pfSense - Bug #7772

Regression of Bug #906

08/14/2017 12:23 PM - Lance Fogle

Status:	Assigned	**Start date:**	08/14/2017
Priority:	Normal	**Due date:**	
Assignee:	Steve Beaver	**% Done:**	0%
Category:	Interfaces	**Estimated time:**	0.00 hour
Target version:	2.5.0		
Affected Version:	2.3.4_1	**Affected Architecture:**	

Description

I read the bug and it says the interface delete code removes firewall rules and that the bug was resolved back in 2010 in version 2.0. I have a firewall that was installed originally with version 2.1 I believe when it started so much later than this bug. It is currently running the latest version (2.3.4-RELEASE-p1) but I can absolutely confirm I see this all the time with firewall rules not being cleaned up. In fact, my current system in question that bothered me enough to open a bug on will not let me delete an alias because it is referenced in one of these "ghost rules."

To give some background on how this came about:
I built new internal LAN CARP pair of firewalls to separate out a physical DMZ where I used to have one unified firewall for LAN and DMZ. Once internal firewall pair was working and routing for the internal LAN, I reconfigured the original single firewall to be an edge firewall so I cleaned up all the LAN interfaces, certificates, aliases (except the one that won't delete), VPN servers, etc and added in the needed static routes and rules on the transit network interface and dmz and all that so that it would serve as the edge.

The firewall rules are obviously still left behind because it is telling me it can't delete the alias because it is referenced by a rule that should no longer exist. Haven't had a chance to look at any code yet but thought I would get the word out there is an issue with the interface deletion code.

History

#1 - 08/14/2017 12:27 PM - Lance Fogle

Please let me know what if any information beyond this you need from me and I will be happy to provide it to help determine the cause. If I end up with some time I will take a look at the code to see if I can contribute as well.

#2 - 08/14/2017 12:31 PM - Lance Fogle

Found this forum post where someone else had an issue with this from deleting VLAN interfaces as well:
https://forum.pfsense.org/index.php?topic=132259.0

#3 - 10/20/2017 09:28 PM - Jim Thompson

- Assignee set to Steve Beaver

- Target version set to 2.4.3

#4 - 02/01/2018 11:09 AM - Steve Beaver

- Status changed from New to Feedback

Can you provide simple steps to reproduce please?

#5 - 02/19/2018 10:52 AM - Lance Fogle

Steve Beaver wrote:

> Can you provide simple steps to reproduce please?

I eventually fixed the issue of the left over rule by exporting the config.xml, removing the invalid rule, then importing back into the firewall with firewall rules selected to be updated. Then I was able to delete the alias which was a known workaround for the original bug.

As far as reproducing, I don't have a test system right now to try to test the ability to reproduce but the implied steps based on the client's setup would be as follows:

Complete inital setup wizard with WAN and LAN interface setup
Create 6 VLANS in interface>vlan tab
Change the LAN interface to use one of those VLANS
Create 5 new OPT interfaces using the remaining VLANs on the same physical interface for the LAN side
Create Host Aliases for destination fields of rules
Create several firewall rules and labels for each interface, with some using the created host aliases in the destination field on each interface
Create one more VLAN (let's call it DMZ)
Create one more OPT interface and assign it to the new DMZ VLAN
Delete all of the original 6 VLAN interfaces on the LAN port leaving only the WAN and new "DMZ" interface (not deleting the labels or firewall rules first)
Try to delete the host aliases that you had created and used previously in the firewall rules

#6 - 03/08/2018 02:52 PM - Jim Pingle

- Status changed from Feedback to Assigned

- Target version changed from 2.4.3 to 2.4.4

#7 - 09/11/2018 01:50 PM - Jim Pingle

- Target version changed from 2.4.4 to 48

#8 - 03/12/2019 10:54 AM - Jim Pingle

- Target version changed from 48 to 2.5.0