pfSense - Feature #6324

Improve IKEv2 multiple traffic selector per SA configuration GUI

05/06/2016 03:38 AM - Jorge Albarenque

Status:	New	**Start date:**	05/06/2016
Priority:	Normal	**Due date:**	
Assignee:	Matthew Smith	**% Done:**	0%
Category:	IPsec	**Estimated time:**	0.00 hour
Target version:	2.5.0		

Description

On IPsec IKEv2 tunnels, by default all defined Ph2s are configured within a single SA.
This could end up with undesired (and potentially security-compromising) settings (I am aware of the option to disable the single SA behavior, it is not my point)

Example:
Ph2 1: 10.0.0.0/24 <-> 192.168.0.0/24
Ph2 2: 10.0.1.0/24 <-> 192.168.1.0/24

This translates to:
leftsubnet = 10.0.0.0/24,10.0.1.0/24
rightsubnet = 192.168.0.0/24,192.168.1.0/24

Which means that 10.0.0.0/24 and 192.168.1.0/24 now have connectivity although no Ph2 is explicitly defined for them, while on IKEv1 with the same settings they don't.

I believe this is a GUI problem. This is the way I think it should behave:

- When IKEv2 with single SA is selected, the GUI should let you create only one Ph2 where you specify all the subnets you want, on both sides, altogether.
- When IKEv2 with split configuration is selected, it should behave as it does right now
- Upgrades from previous versions should default to split configuration to avoid potential security issues.

I also found that this (kind of) breaks the IPsec widget. If you have multiple Ph2s defined with single SA settings, the output doesn't make sense, it shows only one tunnel with single subnets and names (the real problem here is that in fact there is just one SA!). I guess this could be easily fixed with the previous proposed solution.

History

#1 - 05/06/2016 03:49 AM - Chris Buechler

- Tracker changed from Bug to Feature

- Subject changed from IKEv2 multiple traffic selector per SA lead to inappropiate configuration to Improve IKEv2 multiple traffic selector per SA configuration GUI

- Target version changed from 2.3.1 to 2.3.2

The GUI should be as described so it's more clear what you're actually configuring.

#2 - 07/06/2016 04:05 PM - Chris Buechler

- Target version changed from 2.3.2 to 2.4.0

#3 - 01/07/2017 12:34 PM - Jim Thompson

- Assignee set to Matthew Smith

#4 - 09/11/2017 03:58 PM - Renato Botelho

- Target version changed from 2.4.0 to 2.4.1

#5 - 10/12/2017 10:04 AM - Jim Pingle

- Target version changed from 2.4.1 to 2.4.2

#6 - 10/23/2017 12:19 PM - Jim Pingle

- Target version changed from 2.4.2 to 2.4.3

#7 - 03/08/2018 02:36 PM - Jim Pingle

- Target version changed from 2.4.3 to 2.4.4

#8 - 08/14/2018 02:08 PM - Steve Beaver

- Target version changed from 2.4.4 to 48

#9 - 03/12/2019 10:54 AM - Jim Pingle

- Target version changed from 48 to 2.5.0