pfSense - Bug #1560

IPsec GUI needs to reject duplicate subnets in phase 2s for a given phase 1.

05/26/2011 10:48 AM - Jim Pingle

Status:	Resolved	**Start date:**	05/26/2011
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	70%
Category:	IPsec	**Estimated time:**	0.00 hour
Target version:	2.0		
Affected Version:	2.0	**Affected Architecture:**	All

Description

Currently, the GUI lets you specify the same source/destination subnet more than once in the list of phase 2 definitions. This includes listing the same subnet twice in a set of mobile phase 2s. This results in an invalid racoon configuration.

With a site-to-site phase 1, it doesn't appear to prevent racoon from starting but does log an error. With a mobile phase 1 it prevents racoon from starting.

Easy to reproduce by enabling mobile clients, setting up phase 1, and adding the same phase 2 in twice.

Associated revisions

Revision 0c361483 - 12/23/2007 07:47 PM - Scott Ullrich

Remove ipv6 rule reminder statement

Ticket #1560

Revision 061f28bf - 05/31/2011 05:03 AM - Evgeny Yurchenko

Bug #1560. IPsec GUI needs to reject duplicate subnets in phase 2s for a given phase 1(mobile clients).

Revision 538b6eb3 - 05/31/2011 11:41 PM - Evgeny Yurchenko

Bug #1560. IPsec GUI needs to reject duplicate subnets in phase 2s for a given phase 1(site-to-site).

Revision 3da5c50d - 06/01/2011 06:28 PM - Evgeny Yurchenko

Bug #1560.IPsec GUI needs to reject duplicate subnets in phase 2s for a given phase 1 (improvement of previous patch)

Revision b717f1bc - 06/02/2011 11:23 AM - Evgeny Yurchenko

Bug #1560.IPsec GUI needs to reject duplicate subnets in phase 2s for a given phase 1 (fixing p2 edit)

History

#1 - 05/26/2011 01:25 PM - Jim Pingle

Error from the IPsec log:

```
racoon: ERROR: /var/etc/racoon.conf:106: "}" duplicated sainfo: loc='192.168.16.0/24', rmt='ANONYMOUS', peer='
ANY', id=1
```

Looks like mgrooms knew this would be a problem when the new IPsec code went in:
Line 144 of usr/local/www/vpn_ipsec_phase2.php:

```
/* TODO : Validate enabled phase2's are not duplicates */
```

Turns out that if racoon is already running, it will keep running when reloaded with this config, but the tunnel in question doesn't work. If racoon is stopped, it will not start with this config.

#2 - 05/31/2011 11:46 PM - Evgeny Yurchenko

Fixed by https://github.com/bsdperimeter/pfsense/commit/061f28bfd582d1f08d8dfe60f87fc4fd99ec0a93 for mobile clients and by https://github.com/bsdperimeter/pfsense/commit/538b6eb353ce568627513e681483329ecb0d1ec8 for site-to-site.

Need feedback!

PS: racoon gives an error when 'none' is specified in Local Network of phase2 for site-to-site phase1. Should be fixed as new bug?

#3 - 06/01/2011 06:52 AM - Ermal Luçi

- Status changed from New to Feedback

#4 - 06/01/2011 05:02 PM - Jim Pingle

- Status changed from Feedback to New

- % Done changed from 0 to 70

Still at least one case that needs checking:
It still allows you to overlap if you use the "[Interface Name] subnet" drop-down choice and also manually entering the same subnet. So if you have 192.168.16.x for LAN, and you make one p2 with "LAN Subnet" chosen and one with "192.168.16.0/24", it's allowed.

Also if the IP on the subnet isn't the proper subnet boundary it's also allowed. Not sure how racoon likes that anyhow. (192.168.16.0/24 and 192.168.16.5/24 are passed through the GUI checks).

The other cases appear to reject properly now though, where the same choices are used or identical IPs are entered.

#5 - 06/01/2011 05:20 PM - Evgeny Yurchenko

Is 192.168.16.5/24 input considered valid? It's easier to error on this in gui...

#6 - 06/02/2011 09:39 AM - Evgeny Yurchenko

Corrected https://github.com/bsdperimeter/pfsense/commit/3da5c50d5c2285b439a56ab4fcd6f9dbe94f5c4e
Currently there is no check for subnet mask correctness. Whatever user enter goes into racoon.conf. The only check done is new Phase2 specification (networks) should be different from existing ones for given Phase1. Given this racoon neither dies nor reports errors.
Need feedback.

#7 - 06/02/2011 06:11 PM - Evgeny Yurchenko

Jim P noticed that it is impossible now to edit P2, when you change something else rather than networks definitions it will report networks duplication and does not allow to save. This commit https://github.com/bsdperimeter/pfsense/commit/b717f1bc62decb9a02404d427742c352b2b3fbec fixes this issue.

Thanks Jim!

#8 - 06/03/2011 10:30 AM - Jim Pingle

- Status changed from New to Resolved

Tested a few different scenarios and this seems to be solved all the way around. Thanks!