

## pfSense - Bug #3812

### IPSec validation should prevent phase2 policies(subnets) to include remote peer on it

08/18/2014 05:48 AM - Ermal Luçi

<b>Status:</b>	Resolved	<b>Start date:</b>	08/18/2014
<b>Priority:</b>	Normal	<b>Due date:</b>	
<b>Assignee:</b>	Chris Buechler	<b>% Done:</b>	100%
<b>Category:</b>	IPsec	<b>Estimated time:</b>	0.00 hour
<b>Target version:</b>	2.2	<b>Affected Architecture:</b>	
<b>Affected Version:</b>	All		

#### Description

It would be nice to have validation of phase2 subnets to not include the remote peer of ipsec phase1 to avoid loops after tunnel establishment.

#### Associated revisions

##### Revision 6c3be365 - 11/06/2014 04:36 PM - Chris Buechler

Don't allow P2 local+remote network combinations that overlap with interface+remote-gateway of the P1. Fixes #3812

#### History

##### #1 - 08/18/2014 06:55 AM - Jim Thompson

- Tracker changed from Feature to Bug
- Assignee set to Ermal Luçi
- Target version set to 2.2

##### #2 - 08/18/2014 06:55 AM - Jim Thompson

- Affected Version changed from All to 2.2

##### #3 - 11/06/2014 04:33 PM - Chris Buechler

- Status changed from New to Feedback
- Assignee changed from Ermal Luçi to Chris Buechler
- Affected Version changed from 2.2 to All
- Affected Documentation 0 added

fix pushed and tested, leaving for further testing and confirmation. The check only prevents P2s where the local+remote of the P2 both fall within the interface and remote-gateway of its P1. Seems to work and cover all circumstances where that would be a problem.

##### #4 - 11/06/2014 04:50 PM - Chris Buechler

- % Done changed from 0 to 100

Applied in changeset [6c3be3650008801aaa1579dca67b0588c04b8e18](#).

##### #5 - 11/06/2014 07:23 PM - Chris Buechler

- Status changed from Feedback to Resolved

this is good