pfSense - Bug #5819

Mobile IPsec 'pass out' rules overmatch

01/26/2016 09:21 PM - Chris Buechler

Status:	Resolved	**Start date:**	01/26/2016
Priority:	Normal	**Due date:**	
Assignee:	Chris Buechler	**% Done:**	0%
Category:	IPsec	**Estimated time:**	0.00 hour
Target version:	2.3		
Affected Version:	All	**Affected Architecture:**	

Description

The 'pass out' rules for UDP 500 and 4500 and ESP over-match in mobile IPsec scenarios. The route-to ends up breaking connectivity for hosts on internal networks whose egress IPsec traffic leaves via a different WAN than the one the mobile P1 is bound to. So if you have mobile IPsec on WAN2, and your LAN hosts leave WAN1, when a LAN client tries to connect to an outside IPsec server, it'll end up with WAN1's source IP but leave via WAN2.

The pass out is unnecessary for mobile since it never initiates traffic outbound. The auto-added rules for site to site VPNs match the specific remote endpoint's IP, so they don't overmatch.

Associated revisions

Revision bc3e61c4 - 01/26/2016 09:32 PM - Chris Buechler

Skip 'pass out' rules for mobile IPsec. Ticket #5819

History

#1 - 01/26/2016 09:22 PM - Chris Buechler

- Status changed from Confirmed to Feedback

fixed, leaving for additional testing.

#2 - 01/27/2016 12:13 PM - Chris Buechler

- Status changed from Feedback to Resolved

fixed