pfSense - Bug #10814

OpenVPN UDP multihome fails when connecting to an IP that is not logically closest.

08/04/2020 08:16 AM - Steve Wheeler

Status:	Needs Patch	**Start date:**	08/04/2020
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	OpenVPN	**Estimated time:**	0.00 hour
Target version:	2.5.0		
Affected Version:	2.4.x	**Affected Architecture:**	All

Description

If you connect to the external WAN IP from an OpenVPN client on an internal interface of a pfSense install running an OpenVPN server in UDP multihome mode. it will fail.
The server will reply from the closest interface IP and the client will reject the traffic as it does not come from the IP it connected to.

This is a known bug in FreeBSD:
https://reviews.freebsd.org/D24135

Also documented by OpenVPN:
https://community.openvpn.net/openvpn/ticket/1057

It's possible to work around it by setting the -floating option in the client that allows traffic from any IP once authorized. Or by using TCP, this bug applies only to UDP.

History

#1 - 08/04/2020 08:21 AM - Jim Pingle

- Status changed from New to Needs Patch

#2 - 08/04/2020 08:22 AM - Jim Pingle

- Target version deleted (2.5.0)

#3 - 08/07/2020 02:04 PM - Jim Pingle

- Target version set to 2.5.0

The FreeBSD patch has been merged into head (on FreeBSD), will be MFCd soon so it's probably safe to put a 2.5.0 target back on this.

https://svnweb.freebsd.org/base?view=revision&revision=364018