pfSense - Bug #11793

OpenVPN client starts when CARP VIP is in BACKUP status when bound to Virtual IP aliased to CARP VIP

04/09/2021 08:55 AM - monotype tattoo

Status:	Closed	**Start date:**	04/09/2021
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	100%
Category:	OpenVPN	**Estimated time:**	0.00 hour
Target version:	2.5.2		
Plus Target Version:	21.05	**Affected Version:**	2.5.0
Release Notes:	Default	**Affected Architecture:**	All

Description

If an OpenVPN client is bound to a *virtual IP* which is an *IP Alias* for a *CARP IP*, the OpenVPN client (e.g. ovpnc1) gets started when the parent CARP interface's state is *BACKUP*.

With a site-to-site UDP OpenVPN tunnel where the client sits on a redundant pair of pfSense hosts, this causes the stand-by to steal the OpenVPN connection from the active firewall and as a result, traffic received by the active firewall destined for the OpenVPN tunnel is dropped. This continues until a ping activity timeout occurs and restarts the OpenVPN service on the active firewall. The OpenVPN tunnel will then remain up for some time (usually minutes) until once again, a ping activity timeout occurs and restarts the OpenVPN service on the standby firewall.

With a TCP OpenVPN tunnel, the client on the standby firewall will receive a TCP timeout. However, we think we see some knock-on with TCP tunnel connection quality (dropped packets) whilst the standby firewall's OpenVPN process attempts to make the connection.

I think this statement in openvpn.inc needs changing to also check whether the bound interface is *virtual IP* aliased to a *CARP IP* before proceeding to call restart_openvpn:

```
if (($a_groups[$settings['interface']][0]['vip'] <> "") && (!in_array(get_carp_interface_status(
$a_groups[$settings['interface']][0]['vip']), array("MASTER", ""))))
```

[[https://github.com/pfsense/pfsense/blob/a7086b04cae21ca742fdeefd1019ee1401b6dded/src/etc/inc/openvpn.inc#L1500]]

I am raising this as high priority because it has been a significant issue for us in a production environment where we would ideally use a seperate IP for VPN versus customer traffic (other wise face the peril of colo providers DDOS protection system) and we would ideally keep the number of CARP addresses to a minimum so that we don't have IP addresses failing over independently.

Associated revisions

Revision 70d79766 - 05/12/2021 07:10 AM - Viktor Gurov

Do not start an OpenVPN instance if vip aliased to BACKUP CARP. Fixes #11793

History

#1 - 04/19/2021 04:47 AM - Viktor Gurov

fix:
https://gitlab.netgate.com/pfSense/pfSense/-/merge_requests/219

#2 - 04/19/2021 09:39 AM - Jim Pingle

- Status changed from New to Pull Request Review

- Priority changed from High to Normal

- Target version set to 2.6.0

#3 - 05/11/2021 03:05 PM - Jim Pingle

- Plus Target Version set to 21.05

#4 - 05/12/2021 07:10 AM - Steve Beaver

- Status changed from Pull Request Review to Feedback

#5 - 05/12/2021 07:15 AM - Viktor Gurov

- % Done changed from 0 to 100

Applied in changeset 70d797668245d8070782912d6bcdf0939aea7c62.

#6 - 05/12/2021 02:01 PM - Jim Pingle

- Subject changed from OpenVPN client starts on CARP Backup when bound to Virtual IP aliased to CARP address to OpenVPN client starts in CARP Backup status when bound to Virtual IP aliased to CARP VIP

Updating subject for release notes.

#7 - 05/27/2021 07:56 AM - Jim Pingle

- Target version changed from 2.6.0 to 2.5.2

#8 - 05/27/2021 09:17 AM - Jim Pingle

- Category changed from CARP to OpenVPN

#9 - 05/27/2021 09:17 AM - Jim Pingle

- Subject changed from OpenVPN client starts in CARP Backup status when bound to Virtual IP aliased to CARP VIP to OpenVPN client starts when CARP VIP is in BACKUP status when bound to Virtual IP aliased to CARP VIP

Fixing up subject

#10 - 06/02/2021 01:26 PM - Jim Pingle

- Status changed from Feedback to Closed