pfSense - Bug #11300

WireGuard Gateway Should Monitor the Remote Peer, not the Local Peer.

01/23/2021 08:57 AM - Christian McDonald

Status:	Resolved	**Start date:**	01/23/2021
Priority:	Normal	**Due date:**	
Assignee:	Jim Pingle	**% Done:**	100%
Category:	WireGuard	**Estimated time:**	0.00 hour
Target version:	2.5.0		
Plus Target Version:		**Affected Version:**	2.5.0
Release Notes:	Default	**Affected Architecture:**	

Description

Not sure the value of monitoring the local/self peer on WireGuard gateways. These should monitor the far/remote end. Maybe if the 'Peer Wireguard Address' is configured, this should be the Monitor IP. Or create a checkbox that disables automatic Wireguard gateway generation and allow these to be created manually.

Associated revisions

Revision ed837d48 - 01/25/2021 03:05 PM - Jim Pingle

Attempt to use peer wg address if possible for gateway. Implements #11300

History

#1 - 01/23/2021 09:23 AM - Jim Pingle

- Status changed from New to Rejected

- Target version deleted (2.5.0)

It's not viable, unfortunately. I tried doing it a few different ways but the current behavior is the best so far.

You can always make your own gateway using whatever target you want and disable monitoring/actions for the automatic one.

#2 - 01/23/2021 06:44 PM - Christian McDonald

I guess I'm not familiar enough with the current codebase to follow the reasoning here, but I've created a few manual test gateways and these scenarios seem to work for me.

1. Gateway with the gateway/monitoring address of the remote Wireguard peer address.
2. Gateway with the gateway/monitoring address the Wireguard endpoint address as a non-local gateway.

At least both of these options seem to give some indication as to the status of the tunnel, still testing this.

Either way, I'm trying to load-balance between the two tunnels and not having proper gateway marking causes things to tip over when one of the gateways is offline.

#3 - 01/25/2021 08:01 AM - Jim Pingle

- Assignee set to Jim Pingle

- Target version set to CE-Next

- Affected Version set to 2.5.0

The main problem is that there isn't a way for the gateway system to know a viable remote peer address to monitor.

We could maybe loop through and use the first entry in the Peer WireGuard Address field but that isn't guaranteed to respond or be what the user expects either.

The automatic gateway entry is used to nudge traffic into the VPN interface. From there, WireGuard itself decides how to handle the routing based on keys+Allowed IPs (or in the case of 1:1 tunnels, everything on the interface it sent across).

The actual gateway address is moot -- It can't be used by WireGuard since it's L3 only. You can set it up manually for monitoring, but it doesn't influence where anything is routed.

I'd rather avoid giving the user any false hope about what is possible here, but I'm open to refining how the address is determined.

#4 - 01/25/2021 02:37 PM - Jim Pingle

- Status changed from Rejected to New

- Target version changed from CE-Next to 2.5.0

I thought up a viable way to do it. Not as clean/elegant as I wanted, but it works.

#5 - 01/25/2021 03:15 PM - Jim Pingle

- Status changed from New to Feedback

- % Done changed from 0 to 100

Applied in changeset ed837d48335b1cafdaae3c8320c3a78229e57386.

#6 - 01/26/2021 09:23 AM - Christian McDonald

Nice. Patched up this morning on my boxes and this is looking good so far

#7 - 01/26/2021 03:28 PM - Jim Pingle

- Status changed from Feedback to Resolved

Working as intended on current snapshots, for both IPv4 and IPv6.