pfSense Docs - Todo #11812

Feedback on pfSense Configuration Recipes — Configuring IPv6 Through A Tunnel Broker Service

04/17/2021 10:00 PM - Steve Yates

Status:	New	**Start date:**	04/17/2021
Priority:	Low	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Recipes	**Estimated time:**	0.00 hour
Target version:			

Description

Page: https://docs.netgate.com/pfsense/en/latest/recipes/ipv6-tunnel-broker.html

Feedback:
I set this up tonight and it was 99% fine, I got all the way to my PCs getting IPv6 addresses, pfSense could ping out over IPv6, and test-ipv6.com showed 10/10 from my PC, and I could ping ipv6.google.com from my PC. Bravo on the doc page.

However after more testing I realized that DNS lookups to the LAN IPv6 were failing, and I could not ping the router LAN IPv6. Although there was a pre-existing rule allowing IPv6 from LAN Net to Any, the default block rule was blocking the connection from my PC to LAN IPv6:53. I tried adding other rules allowing to This_Firewall:any and to LAN IPv6:53 UDP but they had no effect, nor did restarting unbound.

A search for similar situations found at least two forum comments suggesting a restart of pfSense fixed similar issues. I restarted pfSense and DNS and pinging began working. **I suggest adding a note at the bottom of the page to restart pfSense if DNS/ICMP/IPv6/etc. are not working as expected** from devices on LAN after the tunnel is configured.

This was on pfSense 2.5.1 (our lone non-Netgate hardware), but one forum comment was from 2016.

I cannot explain why a restart was needed but it definitely fixed everything for me.

(side note, test-ipv6.com is linked from this doc page using HTTP so that site shows a message that it supports HTTPS now)

History

#1 - 04/19/2021 09:37 AM - Jim Pingle

- Category changed from Troubleshooting to Recipes

Most likely the only thing you missed was restarting the DNS Resolver at the end of the process so that it could bind to the newly added IPv6 address(es). It's been a while since I've done one from scratch but that seems like the most likely situation. Rebooting shouldn't be necessary.

#2 - 04/19/2021 09:48 AM - Steve Yates

DNS shouldn't affect pinging the IPv6 LAN IP though? Also why would the default block rule trigger? Could it be pfSense didn't apply the IPv6 allow all rule because IPv6 didn't exist at the time they were read? ("Allow IPv6" was checked, but "IPv6 Configuration Type" on WAN was set to None).

It later occurred to me I could try to disable and enable the GIF interface to see if I can repro it...will try that some evening. Or maybe disable, boot, and enable would be closer.

#3 - 04/19/2021 09:58 AM - Jim Pingle

Ah, I misread that part and only caught that DNS wasn't working. Maybe a forced filter reload would have done it then, but usually one of the other various actions would have triggered that. Hard to say then in that case without trying to replicate it locally. If the default block rule was getting hit then somehow it was failing to match the rules, but without seeing the active pf ruleset from the moment it failed, along with the log message, it's impossible to say for certain.

#4 - 04/19/2021 10:13 AM - Steve Yates

Feel free to tell me to post in the forum, I thought a few times about where to suggest/report this. :)

The block:
Apr 17 21:16:49 LAN [2001:470:xxx:xxx:2117:44f5:98ec:4ba2]:50213 [2001:470:xxx:xxx::1]:53 UDP

The existing rule on LAN was for:
IPv6 *, source LAN Net, dest *, gateway *

I tried adding rules from LAN Net to This Firewall:*, to [2001:470:xxx:xxx::1]:53, etc. Definitely the default rule as I had to check "Log packets matched from the default block rules in the ruleset" to see it logged.

The block was hidden at first because the PCs use our Windows Server DNS, hence the test site passing. At some point I realized I couldn't ping or "dig" the router directly.

I'll experiment a bit and report back; might not be tonight.

#5 - 04/19/2021 10:19 AM - Jim Pingle

I meant the actual pf ruleset not what was in the GUI -- /tmp/rules.debug or "pfctl ~~sr" output.~~ Since obviously what was active at the time it failed didn't match what the GUI rules were intending to do.

#6 - 04/19/2021 08:30 PM - Steve Yates

I disabled the GIF interface, DHCPv6, RA, IPv6 on LAN, and booted. I enabled them again and I could ping it as soon as IPv6 on LAN was enabled and applied. So short of actually deleting all the config to start over that should be pretty close.

If I had somehow managed to, say, save the static IPv6 on LAN but not apply it, then routing would still work over the fe80: address...? Would restarting pfSense then apply the unapplied settings? Though how would the firewall log show [2001:470:xxx:xxx::1]:53 was blocked... (trying to brainstorm here)

Another topic on this page...under "Setup the IPv6 Gateway" (which I think should be 'set up') there is no "Default Gateway" checkbox on the page when editing the IPv6 gateway ("Edit the dynamic IPv6 gateway with the same name as the IPv6 WAN created above") or even the IPv4 gateway. After creation the other day that entry already had the globe marking it as default, and "Default gateway IPv6" was set to Automatic, on the Gateways page. I looked at an SG-2100 with native IPv6 and it also has no "default gateway" checkbox on either gateway. I glossed over that the other day as it was marked default on the Gateways page and routing was working.