pfSense Packages - Bug #8197

BIND UI fails to properly update zone with inline DNSSEC signing enabled

12/12/2017 01:56 AM - Alfred Barnat

Status:	New	**Start date:**	12/12/2017
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	BIND	**Estimated time:**	0.00 hour
Target version:			
Affected Version:		**Affected Architecture:**	

Description

2.4.2-RELEASE with BIND 9.11_9 on SG-4860

Steps to reproduce:
1) Install pfSense 2.4.2-RELEASE and the BIND package, and setup a standard configuration with LAN and WAN port.
2) Disable built-in DNS Resolver and DNS Forwarder packages.
3) Enable BIND and configure it to listen on all interfaces. Confirm BIND responds to requests on the LAN interface IP.
4) Configure a master zone for the domain of your choice, enable inline DNSSEC signing on this zone, and confirm BIND responds to requests for DNS records in this zone.
5) Add a new A record for the host "test" under this zone, with the IP of your choice, and save. At this point, BIND should respond to requests for this host.
6) Remove this host "test", and save. At this point, BIND still responds to requests for the now-deleted record.

I've confirmed that the zone's ".DB" file (in /cf/named/etc/namedb/master/<view>) is correct at this point, but the problem seems to be one or more of the ".DB.jbk", ".DB.signed", and ".DB.signed.jnl" files. Disabling inline DNSSEC signing in the UI will correct the problem with no further action, at the expense of DNSSEC of course. Removing these three files and restarting BIND also appears to correct the problem by causing the files to be regenerated without the now-removed DNS record. Presumably the UI is missing some step that should cause this update to occur in a less destructive manner.

History

#1 - 02/18/2019 05:23 PM - Jared Dillard

- Category set to BIND