pfSense - Bug #9059

Update Unbound to 1.8.1

10/23/2018 08:30 AM - Jim Pingle

Status:	Resolved	**Start date:**	10/23/2018
Priority:	Normal	**Due date:**	
Assignee:	Jim Pingle	**% Done:**	0%
Category:	DNS Resolver	**Estimated time:**	0.00 hour
Target version:	2.4.4-p1		
Affected Version:	2.4.4	**Affected Architecture:**	All

Description

Unbound 1.8.1 has fixed a few memory leaks, notably one in DNS over TLS that causes unbound to consume all memory and fail after a few days.

We need to pull this into devel and have it in -p1 as well. Maybe even have it available for users to pull into 2.4.4, since users are seeing these memory issues and unbound failures in production setups.

https://nlnetlabs.nl/pipermail/unbound-users/2018-October/010992.html

History

#1 - 10/30/2018 07:52 AM - Jim Pingle

- Status changed from New to In Progress

- Assignee changed from Renato Botelho to Jim Pingle

Cherry picked a270651cc45b428b5f8167d1d533c50e5ee958c2 to devel. If it's OK on 2.4.5 we can consider picking it back to RELENG_2_4_4 early to help with the memory leaks.

#2 - 11/07/2018 12:27 PM - Jim Pingle

- Status changed from In Progress to Resolved

This was picked back to 2.4.4 last week. Looks good, no complaints or errors encountered.

#3 - 12/03/2018 04:22 PM - Isaac McDonald

I updated Unbound to 1.8.1

pkg update; pkg upgrade unbound

After the upgrade I found that Unbound appears to only be using a single thread. Note that only "thread 0" has any stats

>unbound-control -c /var/unbound/unbound.conf stats_noreset

thread0.num.queries=1997
thread0.num.queries_ip_ratelimited=0
thread0.num.cachehits=21
thread0.num.cachemiss=1976
thread0.num.prefetch=3
thread0.num.zero_ttl=7
thread0.num.recursivereplies=1943
thread0.requestlist.avg=18.0273
thread0.requestlist.max=55
thread0.requestlist.overwritten=0
thread0.requestlist.exceeded=0
thread0.requestlist.current.all=25
thread0.requestlist.current.user=18
thread0.recursion.time.avg=0.360357
thread0.recursion.time.median=0.16633
thread0.tcpusage=0

thread1.num.queries=0
thread1.num.queries_ip_ratelimited=0
thread1.num.cachehits=0
thread1.num.cachemiss=0
thread1.num.prefetch=0
thread1.num.zero_ttl=0
thread1.num.recursivereplies=0
thread1.requestlist.avg=0
thread1.requestlist.max=0
thread1.requestlist.overwritten=0
thread1.requestlist.exceeded=0
thread1.requestlist.current.all=0
thread1.requestlist.current.user=0
thread1.recursion.time.avg=0.000000
thread1.recursion.time.median=0
thread1.tcpusage=0
thread2.num.queries=0
thread2.num.queries_ip_ratelimited=0
thread2.num.cachehits=0
thread2.num.cachemiss=0
thread2.num.prefetch=0
thread2.num.zero_ttl=0
thread2.num.recursivereplies=0
thread2.requestlist.avg=0
thread2.requestlist.max=0
thread2.requestlist.overwritten=0
thread2.requestlist.exceeded=0
thread2.requestlist.current.all=0
thread2.requestlist.current.user=0
thread2.recursion.time.avg=0.000000
thread2.recursion.time.median=0
thread2.tcpusage=0
thread3.num.queries=0
thread3.num.queries_ip_ratelimited=0
thread3.num.cachehits=0
thread3.num.cachemiss=0
thread3.num.prefetch=0
thread3.num.zero_ttl=0
thread3.num.recursivereplies=0
thread3.requestlist.avg=0
thread3.requestlist.max=0
thread3.requestlist.overwritten=0
thread3.requestlist.exceeded=0
thread3.requestlist.current.all=0
thread3.requestlist.current.user=0
thread3.recursion.time.avg=0.000000
thread3.recursion.time.median=0
thread3.tcpusage=0
total.num.queries=1997
total.num.queries_ip_ratelimited=0
total.num.cachehits=21
total.num.cachemiss=1976
total.num.prefetch=3
total.num.zero_ttl=7
total.num.recursivereplies=1943
total.requestlist.avg=18.0273
total.requestlist.max=55
total.requestlist.overwritten=0
total.requestlist.exceeded=0
total.requestlist.current.all=25
total.requestlist.current.user=18

Can you confirm that all threads are being used to process traffic in 1.8.1?

PS: This bug can result in a denial of service due to pfSense running out of memory. This update needs to be released sooner rather than later.

#4 - 12/03/2018 04:38 PM - Tim Harman

I can confirm I see the same after 2.4.4-p1

```
thread0.num.queries=6309
thread0.num.queries_ip_ratelimited=0
thread1.num.queries=0
thread1.num.queries_ip_ratelimited=0
total.num.queries=6309
total.num.queries_ip_ratelimited=0
```

That said, I don't have a previous record of this to state if it ever worked.

I only have 2 CPUs in this box, I assume that's why I don't see a "thread 3" as Isaac does.

#5 - 12/03/2018 04:45 PM - Tim Harman

I found this on the unbound mailing list: https://nlnetlabs.nl/pipermail/unbound-users/2018-October/010991.html

> I expected this to be related to so-reuseport and after setting that to 'no',
> things were back to normal (all threads handled queries again, queue size back to normal).

The also state it will be fixed 1.8.2
I tried setting this knob in custom settings but it gave me an error (and the doco for so-reuseport states it's a Linux only feature)

#6 - 12/03/2018 04:53 PM - Tim Harman

I'm an idiot.

```
server:
so-reuseport: no
```

In custom options works just fine.

It resolves the issue:

```
thread0.num.queries=34
thread0.num.queries_ip_ratelimited=0
thread1.num.queries=50
thread1.num.queries_ip_ratelimited=0
total.num.queries=84
```

#7 - 12/03/2018 05:08 PM - Isaac McDonald

Did this make it into 2.4.4_1 ?

#8 - 12/03/2018 05:11 PM - Tim Harman

Isaac McDonald wrote:

> Did this make it into 2.4.4_1 ?

Huh? We're discussing the bug right now, so I can't see how unless we went back in time :-)

Unbound 1.8.1 is part of 2.4.4-p1 (though it's actually been a released pfSense package for about a month).
I guess it might make sense for the pfSense team to roll out an updated 1.8.1 package with this flag set, but as of right now this "bug" still exists. You need to add the workaround in my previous comment to fix it.

#9 - 12/03/2018 05:21 PM - Isaac McDonald

I was asking if:

server:
so-reuseport: no

was set in 2.4.4-p1. I guess the answer is no it did not. This is especially frustrating seeing as how I reported this issue several days ago via the forum. I'll use the bug tracker next time.

#10 - 12/09/2018 09:06 AM - Darin May

Tim Harman wrote:

> I'm an idiot.

Been there, done that.

Should the advanced config be entered as two separate lines or concatenated together as in the existing entry in advanced settings?

```
server:include: /var/unbound/pfb_dnsbl.*conf
```

So it looks like:

```
server:so-reuseport: no
```

Or should it be as written:

```
server:
```

```
so-reuseport: no
```

Are they equivalent? I'm unfamiliar with the settings notation if it matters or not.

#11 - 12/11/2018 03:54 PM - Ben Hohendorf

As per my thread on reddit, https://www.reddit.com/r/PFSENSE/comments/9wjjo2/sg3100_hard_crash/

After updating my sg3100 to the latest 2.4.4-RELEASE-p1,i re enabled Use SSL/TLS for outgoing DNS Queries to Forwarding Servers.
My box then did the typical hard crash after a day.

Let me know if you need anything to help debug this.

#12 - 12/11/2018 04:27 PM - Tim Harman

Ben Hohendorf wrote:

> As per my thread on reddit, https://www.reddit.com/r/PFSENSE/comments/9wjjo2/sg3100_hard_crash/
>
> After updating my sg3100 to the latest 2.4.4-RELEASE-p1,i re enabled Use SSL/TLS for outgoing DNS Queries to Forwarding Servers.
> My box then did the typical hard crash after a day.
>
> Let me know if you need anything to help debug this.

Ben you could try the

```
server:
so-reuseport: no
```

in the advanced settings? As Isaac McDonald suggests, the lack of being threaded can cause a DoS (But note I have NO basis/evidence to support that claim!)

Regardless, this bug probably is not the right place to discuss your problems - I would go back to the forums and if a concrete reason for the problems you're experiencing can be found, another ticket specific to that issue should be raised.