pfSense - Bug #8971

filterdns doesn't start after upgrade from 2.4.3 to 2.4.4

09/27/2018 06:21 PM - Adrien Carlyle

Status:	Not a Bug		Start date:	09/27/2018
Priority:	Normal		Due date:	
Assignee:			% Done:	0%
Category:	FilterDNS		Estimated time:	0.00 hour
Target version:				
Affected Version:	2.4.4		Affected Architecture:	All

Description

After upgrading firewalls to 2.4.4 I'm noticing that any FW rules which use an alias with an FQDN name are not working. I'm noticing this on a bare metal CE install as well as the SG-3100 and GS-1000 units I have deployed.

On the forums I was able to track this down to the filterdns process. It appears the filterdns process isn't running at all after a reboot, and nothing is logged like I would expect under Status -> System Logs -> DNS Resolver. I am unable to launch it manually via the cli. I am also unable to see the expanded contents of the aliases affected under diagnostics / tables.

Please let me know if I can provide any more details from my systems to assist.

History

#1 - 09/27/2018 08:02 PM - Tim Harman

I can't reproduce this on my setup (2.4.4 running x64 under KVM)

I added a test host, added a rule that allowed it and logged it.
I see it allowed in the firewall, I see packets incrementing, and more importantly in the status_logs.php?logfile=resolver of the firewall I see:

```
Sep 28 12:55:19    filterdns       adding entry 103.247.152.88 to pf table testing for host tjharman.com
Sep 28 12:56:08    filterdns       clearing entry 103.247.152.88 from pf table testing on host tjharman.com
Sep 28 12:56:08    filterdns       adding entry 103.247.152.88 to pf table testing for host tjharman.com
Sep 28 12:56:26    filterdns       clearing entry 103.247.152.88 from pf table testing on host tjharman.com
Sep 28 12:56:26    filterdns       adding entry 103.247.152.88 to pf table testing for host tjharman.com
```

I also see the following processes running

```
[2.4.4-RELEASE][admin@fw]/usr/local/sbin: ps afux | grep filter
root    21568   0.0  0.3  8712  2668  -  Is   12:55      0:00.00 /usr/local/sbin/filterdns -p /var/run/filterd
ns.pid -i 300 -c /var/etc/filterdns.conf -d 1
root    37155   0.0  0.2  6604  2364  -  Ss   Wed14      0:04.69 /usr/local/sbin/filterlog -i pflog0 -p /var/r
un/filterlog.pid
```

What if you manually edit the alias table and re-save it. Does that trigger filterdns to load? (I'm unable to reboot my FW at the moment to see if filterdns starts automatically)
Note that before I did this test, I wasn't using any FQDN entries, so filterdns wasn't required for me.

#2 - 09/27/2018 08:21 PM - Adrien Carlyle

I can add that I'm running 1 CE instance in a VM that appears to have the process running but it's filterdns process looks a bit different than the one you posted here. But all installations that are on bare metal seem to have this issue for me.

Yes I don't see any counts on my rules and no output for filterdns in the resolver log.

On one 2.4.4 system I even added an fqdn rule from scratch, and filterdns was not started to handle creating the new rule.

#3 - 09/27/2018 08:24 PM - Tim Harman

Adrien Carlyle wrote:

> I can add that I'm running 1 CE instance in a VM that appears to have the process running but it's filterdns process looks a bit different than the one you posted here. But all installations that are on bare metal seem to have this issue for me.
>
> Yes I don't see any counts on my rules and no output for filterdns in the resolver log.
>
> On one 2.4.4 system I even added an fqdn rule from scratch, and filterdns was not started to handle creating the new rule.

Maybe it is an ARM issue (the SG-3100 and SG-1000 are both ARM based)

#4 - 09/27/2018 08:39 PM - Adrien Carlyle

I'm not too sure on that, I'm running an intel based system here at my house which has similar problems.

Actually, I've just checked my VM and while I have filterdns entries in the log updating the rules, there is no actual filterdns process running on the system using the command you showed.

#5 - 09/28/2018 08:07 AM - Adrien Carlyle

So on my SG-3100, I tried to run the process manually and the following output happens.

```
[2.4.4-RELEASE][admin@pfsense]/root: whoami
root
[2.4.4-RELEASE][admin@pfsense]/root: /usr/local/sbin/filterdns -p /var/run/filterdns.pid -i 300 -c /var/etc/fi
lterdns.conf -d 1
filterdns: open file
[2.4.4-RELEASE][admin@pfsense]/root: ps afux | grep filter
root    41616  0.0  0.1  6204  2008  0  S+  13:50      0:00.00 grep filter
[2.4.4-RELEASE][admin@pfEdge-office.kortext.local]/root: cat /var/run/filterdns.pid
cat: /var/run/filterdns.pid: No such file or directory
[2.4.4-RELEASE][admin@pfsense]/root: cat /var/etc/filterdns.conf
cat: /var/etc/filterdns.conf: No such file or directory
[2.4.4-RELEASE][admin@pfsense]/root:
```

On my CE install on intel cpu.

```
[2.4.4-RELEASE][admin@pfsense]/root: whoami
root
[2.4.4-RELEASE][admin@pfsense]/root: ps afux | grep filter
root    14195   0.0  0.0  6564  2456  0  S+   08:57     0:00.00 grep filter
[2.4.4-RELEASE][admin@pfsense]/root: /usr/local/sbin/filterdns -p /var/run/filterdns.pid -i 300 -c /var/etc/fi
lterdns.conf -d 1
filterdns: open file
[2.4.4-RELEASE][admin@pfsense]/root: cat /var/run/filterdns.pid
cat: /var/run/filterdns.pid: No such file or directory
[2.4.4-RELEASE][admin@pfsense]/root: cat /var/etc/filterdns.conf
cat: /var/etc/filterdns.conf: No such file or directory
[2.4.4-RELEASE][admin@pfsense]/root:
```

On both of these systems, if I create a rule that uses an alias that has a fqdn, the filterlog process does start, but filterdns never starts. I have attempted to manually create the pid/conf files, but the process still will not launch, and upon reboot the files are deleted.

#6 - 09/28/2018 08:11 AM - Adrien Carlyle

Adrien Carlyle wrote:

> I can add that I'm running 1 CE instance in a VM that appears to have the process running but it's filterdns process looks a bit different than the one you posted here. But all installations that are on bare metal seem to have this issue for me.
>
> Yes I don't see any counts on my rules and no output for filterdns in the resolver log.
>
> On one 2.4.4 system I even added an fqdn rule from scratch, and filterdns was not started to handle creating the new rule.

I was completely wrong and made a mistake in stating that I was seeing the process run on this system, I was seeing the "filterlog" process on that system, filterdns won't launch/run on that system either and the last updates I see from it for the DNS rules are from just before the upgrade from 2.4.3 to 2.4.4.

#7 - 09/28/2018 09:33 AM - Jim Pingle

- Status changed from New to Feedback

I do not believe this is a widespread problem. In part due to the fact that if it were, we'd see a lot more feedback about it.

I have 20 systems in my lab (including my edge firewall) and I can't reproduce this on any of them. 4 of these had filterdns running already and have been upgraded across various old versions but are now on 2.4.4 or 2.4.5 (some of each). I added a new alias to all of them which included a hostname, and then used that alias in a rule, and then checked the result. filterdns is running on all of them, the config is populated, the table has the resolved address. There are lots of variations across this lab. Multiple architectures (VMs, bare metal, ARM on SG-1000s and 3100s, even a new aarch64 box) and variations between using the DNS forwarder and resolver and their configuration.

So either this is something specific to your configuration or your environment. The fact that you do not have a filterdns.conf file present makes me think it's skipping that process for some reason, perhaps because your firewall is crashing or has an error on the console that prevents it from fully booting properly. If the firewall believes it is still booting, it will not write out the filterdns config. Look for /var/run/booting and see if the file is still present. If so, attach to the console, reboot the firewall, and see why it is not completing the boot process.

#8 - 09/28/2018 10:40 AM - Adrien Carlyle

- File IMG_20180928_113702.jpg added

On my CE system running in a VM, /var/run/booting does not exist. filterdns did not show up in processes.   when saving a firewall rule containing an fqdn based rule, the filter processes are now running as expected. So this looks good, which is fantastic. And I do remember that I had to manually delete /var/run/booting on a system becuase I was having an issue trying to configure something around a week ago.

```
root    14702  0.0  0.1  6916  2724  -  Is   Thu04      0:00.14 /usr/local/sbin/filterdns -p /var/run/filterdn
s.pid -i 300 -c /var/etc/filterdns.conf -d 1
root    49389  0.0  0.1  6600  2608  -  Ss   Thu04      0:36.59 /usr/local/sbin/filterlog -i pflog0 -p /var/ru
n/filterlog.pid
root    75474  0.0  0.1  6660  2600  -  Is   Thu04      0:00.57 /usr/local/sbin/filterdns -p /var/run/filterdn
s-ipsec.pid -i 60 -c /var/etc/ipsec/filterdns-ipsec.hosts -d 1
root    11655  0.0  0.0   408   324  0  R+   16:17      0:00.00 grep filter
```

On the system in my house (ce on intel mini server), /var/run/booting exists. so filterdns isn't running as expected. I manually deleted it, rebooted the system, boot looks clean (attached), but /var/run/booting remains on disk.   What else can I check to see why the boot might not be completing?

On the SG-3100 (8 hour flight away) /var/run/booting exists, and filterdns isn't working. This may also explain why my IPsec service needs manually started after every boot.   Is there any way to view a boot log remotely to see why it isn't completing the process and clearing this file?

#9 - 09/28/2018 10:50 AM - Jim Pingle

- Status changed from Feedback to Not a Bug

- Target version deleted (2.4.4-GS)

OK, so your issue is not with filterdns, and this is not a bug, it's a side effect of your real root issue.

We can continue the discussion on the forum to figure out why your systems are not completing the boot process. You will most likely need to attach

to the console and monitor the boot process to find out why.

This could be from any number of things, but usually it's from custom startup scripts not exiting properly or a similar problem from packages. Something on those boxes is failing to complete or causing an error which makes the boot process fail to fully complete. If you have any custom shellcmd entries I'd look at those first.

#10 - 09/30/2018 07:38 AM - Sandy Kim

Not sure if this is the best place to post, but the symptom in the original poster's screenshot is also what we're seeing and this was the only related item we could find. In short, our DNS doesn't work after upgrading to 2.4.4.

1.   On our bare metal install, we updated pfsense from 2.4.3 to 2.4.4, it seemed to go ok.

2.   But when we rebooted the final time, it said:
Setting up static routes…done.
Setting up DNSs…
Starting DNS Resolver…done.
…
Bootup complete

In the long list on the VGA console screen, everything seemed good except "Setting up DNSs" is not done.

3.   Checking some of the other things mentioned in this thread:
[2.4.4-RELEASE][root@pfsense.localadmin]/usr/local/sbin: ps afux -w | grep filter
(added w to display more, otherwise ps cut the line short after about …/sbin/ - even with using w, though, the first line seems to cut off because it is over 132 columns, not sure how to get more to display)
root   21568 0.0 0.3 8712 2668 - Is   12:55   0:00.00 /usr/local/sbin/filterdns -p /var/run/filterdns.pid -i 300 -c /var/
root   36093 0.0 0.1 6600 2340 - Ss   13:38   0:00.72 /usr/local/sbin/filterlog -i pflog0 -p /var/run/filterlog.pid

4.   The booting file doesn't exist. (/var/run/booting)

5.   We don't use any scripts or packages, just a small office routing everything through an OpenVPN client.

6.   Status > Gateways > Gateways: status of WAN is online, but status of VPN is pending.

7.   Status > OpenVPN: Status of client is "reconnecting; init_instance" and the Local address and remote host is "pending".

8.   Diagnostics > Ping: if put in a hostname, it immediately says "host "domain.com" did not respond or could not be resolved. But ip addresses work.

9.   Is there anything else we should check or any other information we can send to understand what might be going on here?

Thank you!

PS, In the meantime we're thinking of trying to install back to 2.4.3, but they seem to be gone from the mirrors, is there a way to still download copy?

#11 - 09/30/2018 08:19 AM - Jim Pingle

Your issue is different. You need to start a thread on the [forum](#) to discuss it and diagnose the issue and get assistance with your other questions.

Files

IMG_20180928_113702.jpg	4 MB	09/28/2018	Adrien Carlyle