

pfSense - Bug #7884

Unbound refusing non-recursive/iterative queries even from localhost

09/21/2017 09:42 AM - Kill Bill

Status:	Resolved	Start date:	09/21/2017
Priority:	Low	Due date:	
Assignee:		% Done:	0%
Category:	DNS Resolver	Estimated time:	0.00 hour
Target version:	2.4.1	Affected Architecture:	All
Affected Version:	All		

Description

This is so much secure that it's annoying and getting in the way of normal work for not exactly any good reason.

```
# dig www.google.com +trace
; <<>> DiG 9.11.2 <<>> www.google.com +trace
;; global options: +cmd
;; Received 12 bytes from 127.0.0.1#53(127.0.0.1) in 0 ms
```

Wonderful and very "useful". So what's really going on is this:

```
# dig ns . +norecur
; <<>> DiG 9.11.2 <<>> ns . +norecur
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 57656
;; flags: qr ad; QUERY: 0, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0
;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Thu Sep 21 16:40:09 CEST 2017
;; MSG SIZE rcvd: 12
```

Suggested fix for more useful default ACLs for localhost available @ <https://github.com/pfsense/pfsense/pull/3826>

History

#1 - 09/21/2017 11:13 AM - Jim Pingle

- Status changed from New to Confirmed

PR looks good and the change lets dig +trace and drill -T work locally.

#2 - 10/16/2017 03:34 PM - James Dekker

On pfSense-netgate-memstick-ADI-2.4.1-DEVELOPMENT-amd64-20171016-1127.img "dig google.com +trace" and "drill -T google.com" both succeed.

#3 - 10/16/2017 03:42 PM - Jim Pingle

- Status changed from Confirmed to Resolved