pfSense - Bug #6065

unbound: Domain Overrides are not always working if using stub-zones

04/02/2016 08:05 PM - Grischa Zengel

Status:	Resolved	**Start date:**	04/02/2016
Priority:	Normal	**Due date:**	
Assignee:	Chris Buechler	**% Done:**	0%
Category:	DNS Resolver	**Estimated time:**	0.00 hour
Target version:	2.3.1		
Affected Version:	All	**Affected Architecture:**	

Description

The most time Domain Overrides are used for private networks:

1. The used DNS servers are not authoritative
2. The authoritative DNS Servers are in not reachable subnets so recursive queries are not possible

I found this https://wiki.archlinux.org/index.php/Unbound:

> Note: There is a difference between forward zones and stub zones - stub zones will only work when connected to an authoritative DNS server directly. This would work for lookups from a BIND DNS server if it is providing authoritative DNS - but if you are referring queries to an unbound server in which internal lookups are forwarded on to another DNS server, then defining the referral as a stub zone in the machine here will not work. In that case it is necessary to define a forward zone as above, since forward zones can have daisy chain lookups onward to other DNS servers. i.e. forward zones can refer queries to recursive DNS servers. This distinction is important as you do not get any error messages indicating what the problem is if you use a stub zone inappropriately.

1. Use domain-insecure if DNSSEC is enabled
2. Use forward-zone instead of stub-zone
3. I have learned to put a point after FQDN

This works very well:

```
domain-insecure: "extern1.local."
domain-insecure: "hq1.local."
domain-insecure: "hq2.local."
forward-zone:
        name: "extern1.local."
        forward-addr: 10.190.0.1
forward-zone:
        name: "hq1.local."
        forward-addr: 10.190.0.1
forward-zone:
        name: "hq2.local."
        forward-addr: 10.190.0.1
```

Associated revisions

Revision 0bde07b7 - 04/21/2016 03:22 AM - Chris Buechler

Switch domain overrides from stub-zone to forward-zone. Ticket #6065

Revision 6ecf66a9 - 04/21/2016 03:23 AM - Chris Buechler

Switch domain overrides from stub-zone to forward-zone. Ticket #6065

History

#1 - 04/02/2016 08:25 PM - Grischa Zengel

I forgot. From man page:

> The servers listed as forward-host: and forward-addr: have to handle further recursion for the query. Thus, those servers are not authority servers, but are (just like unbound is) recursive servers too; unbound does not perform recursion itself for the forward zone, it lets the remote server do it.

#2 - 04/02/2016 08:59 PM - Chris Buechler

- Status changed from New to Confirmed

- Assignee set to Chris Buechler

- Priority changed from Normal to Low

- Target version changed from 2.3 to 2.3.1

- Affected Version changed from 2.3 to All

It looks like it would be preferable to use forward-zone rather than stub-zone in all cases for domain overrides. The only diff appears to be that stub-zones only work if the target IP is authoritative for the domain in question (which is almost always true for domain overrides), where forward-zone has no such requirement.

I don't see any possibilities for regressions by changing it, but not doing so at this point in 2.3 given it works as-is for nearly every use case and it's the same as it's always been.

#3 - 04/03/2016 06:54 AM - Grischa Zengel

> which is almost always true for domain overrides

I don't agree.

1. I use domain overrides as an on-site alias to DNS servers, so I don't have to communicate DNS server moves or have to change a lot of off-site pfsenses.
2. I have multi-site domains and only add on-site DNS servers because the most DNS servers are not reachable or you have unwanted traffic over WAN.
   - DNS clients only know local DNS server. Stub-zones queries goes everywhere even to forgotten DNS servers.

#4 - 04/21/2016 03:27 AM - Chris Buechler

- Status changed from Confirmed to Feedback

- Priority changed from Low to Normal

ran into a situation with a support customer where forward-zone was necessary. stub-zone can be problematic in a variety of circumstances, and I don't see any situation for our use cases where it would be preferable. Can still be configured as advanced options if anyone wants.

I pushed a change to use forward-zone instead of stub-zone for domain overrides.

#5 - 04/21/2016 07:56 AM - Daniel Weeber

Had a hard time figuring out I had to insert "domain-insure :"domain.local" for a domain I had a Domain Override for (and DNSSEC enabled).
In my opinion this should either happen automatically when adding a domain override or there should be a checkbox for that?

#6 - 04/22/2016 02:43 AM - Chris Buechler

- Status changed from Feedback to Resolved

Fixed.

Daniel Weeber wrote:

> Had a hard time figuring out I had to insert "domain-insure :"domain.local" for a domain I had a Domain Override for (and DNSSEC enabled).
> In my opinion this should either happen automatically when adding a domain override or there should be a checkbox for that?

It's often not necessary to disable DNSSEC for forwarded domains, so not something to be done by default. Might be worth a checkbox in domain overrides at some point. It's easy enough to manually configure.