

pfSense - Feature #8028

Unbound: Add advanced option for qname-minimization

10/30/2017 11:30 AM - Mathew Keith

Status:	Resolved	Start date:	10/30/2017
Priority:	Normal	Due date:	
Assignee:	Jim Pingle	% Done:	100%
Category:	DNS Resolver	Estimated time:	0.00 hour
Target version:	2.4.4		
Description			
Add support for qname-minimization and maybe qname-minimisation-strict.			
This can be implemented in two ways, depending on if only qname-minimization or both qname-minimization-strict is implemented.			
1) Only qname-minimization:			
Add a checkbox to the Advanced settings:			
Label: aname Minimization			
Description: Send minimum amount of information to upstream servers to enhance privacy. Best effort.			
If checked, add the following to unbound's config:			
qname-minimisation: yes			
2) Both qname-minimization and qname-minimization-strict.			
Add a dropdown to the Advanced settings			
Label: qname mimization			
Dropdown options:			
Disabled			
Enabled			
Strict			
Description: Send minimum amount of information to upstream servers to enhance privacy. Only use Strict if you know what you are doing.			
If enabled add the following to the unbound config:			
qname-minimisation: yes			
If Strict add the following to the unbound config:			
qname-minimisation: yes			
qname-minimisation-strict: yes			

Associated revisions

Revision 547e51b8 - 04/04/2018 12:36 PM - Jim Pingle

Add query name minimization options to DNS Resolver. Implements #8028

History

#1 - 11/02/2017 11:20 AM - Mathew Keith

RFC spec here:

<https://tools.ietf.org/html/rfc7816>

Should this be ignored if forwarding mode is enabled? I don't know if it will continue making incrementally more precise queries if forwarding.

#2 - 11/02/2017 12:19 PM - JohnPoz _

I have been using the

qname-minimisation: yes

Option via adding it to custom option box for a few days now and have not seen any adverse effects. I will also enable the strict and see if run into any issues with it.

#3 - 11/02/2017 10:23 PM - Jim Thompson

- Assignee set to Steve Beaver

#4 - 11/04/2017 03:17 AM - JohnPoz _

Well if going to add options for the -strict in the gui... Needs to have BIG note on it that it WILL BREAK stuff... None of the Microsoft stuff is working that points edgekey and akamai domains

Example, this will not resolve with the -strict option in play.

;; ANSWER SECTION:

```
blogs.technet.microsoft.com. 3599 IN CNAME blogs.technet.microsoft.com.edgekey.net.  
blogs.technet.microsoft.com.edgekey.net. 21600 IN CNAME e8798.b.akamaiedge.net.  
e8798.b.akamaiedge.net. 3600 IN A 23.222.137.74
```

Seems like all of the ms records that do this sort of thing are broken...

#5 - 11/04/2017 07:41 AM - Mathew Keith

I don't think strict should be an option through the GUI now that I've played with it.

With respect to qname-minimisation and forwarding mode, I receive syntax errors when using both together. Perhaps this can be ignored when forwarding mode is enabled with a note indicating that it only applies when forwarding is disabled.

#6 - 04/04/2018 07:42 AM - Jim Pingle

- Project changed from pfSense Packages to pfSense
- Category changed from Unbound to DNS Resolver
- Assignee changed from Steve Beaver to Jim Pingle
- Target version set to 2.4.4

#7 - 04/04/2018 12:50 PM - Jim Pingle

- Status changed from New to Feedback
- % Done changed from 0 to 100

Applied in changeset [547e51b887a88d97569e587de26e029674c5d5f0](#).

#8 - 04/06/2018 01:00 PM - Jim Pingle

- Status changed from Feedback to Resolved

Works