pfSense - Feature #8388

Add DNS over TLS for upstream forwarders to the DNS Resolver

03/24/2018 08:22 AM - Joe Gassner

Status:	Resolved	**Start date:**	04/04/2018
Priority:	Low	**Due date:**	
Assignee:	Jim Pingle	**% Done:**	100%
Category:	DNS Resolver	**Estimated time:**	0.00 hour
Target version:	2.4.4		
Plus Target Version:		**Release Notes:**	Default

Description

GUI options to set DNS over TLS.

Currently you can do this by adding a stanza to the custom options on unbound.

```
server:
ssl-upstream: yes
do-tcp: yes
forward-zone:
    name: "."
    # Below 3 addresses are Quad9 resolvers
    forward-addr: 9.9.9.9@853
    forward-addr: 149.112.112.112@853
    forward-addr: 2620:fe::fe@853
```

Subtasks:

Feature # 8431: Add DNS over TLS checkbox for Domain Override entries	**Resolved**

Associated revisions

Revision cd738219 - 04/04/2018 10:01 AM - Jim Pingle

Add GUI option for DNS over TLS. Implements #8388

History

#1 - 04/04/2018 07:41 AM - Jim Pingle

- Status changed from New to Duplicate

Duplicate of #8030

#2 - 04/04/2018 08:19 AM - Jim Pingle

- Category set to DNS Resolver

- Status changed from Duplicate to Assigned

- Assignee set to Jim Pingle

- Target version set to 2.4.4

On second thought, this is different. The other ticket is for providing DNS over TLS to local clients, this is for upstream forwarders. Reopening.

See also: #8415

#3 - 04/04/2018 08:21 AM - Jim Pingle

- Subject changed from DNS over TLS to Add DNS over TLS for upstream forwarders to the DNS Resolver

#4 - 04/04/2018 10:10 AM - Jim Pingle

- Status changed from Assigned to Feedback

- % Done changed from 0 to 100

Applied in changeset cd73821986dd854afbff4b1f63c7fa2bc88ed9a2.

#5 - 04/04/2018 10:48 AM - Jim Pingle

- % Done changed from 100 to 0

Of note, a couple changes compared to other examples:

1. We already set do-tcp: yes, so adding it again was unnecessary
2. Using ssl-upstream will cause all outgoing queries to use TLS, not just forwards, which could break Domain Overrides, so I used forward-tls-upstream instead inside the '.' zone which will only apply the TLS setting to that forwarding zone.
3. Unbound is moving the ssl keywords to tls instead, so the patch will only work as-is on 2.4.4 which has Unbound 1.7. For 2.4.3 and before, use forward-ssl-upstream

#6 - 04/06/2018 01:00 PM - Jim Pingle

- Status changed from Feedback to Resolved

Works.