DNS-over-TCP/TLS Implementation

Sara Dickinson
Sinodun

DNSOP@IETF96           Berlin, July 2016
# Recursive implementations

<table>
<thead>
<tr>
<th>Features</th>
<th>TCP/TLS Features</th>
<th>TLS Features</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>TCP fast open</td>
<td>TLS on port 853</td>
</tr>
<tr>
<td></td>
<td>Process pipelined queries</td>
<td>Provide server certificate</td>
</tr>
<tr>
<td></td>
<td>Provide OOOR</td>
<td>EDNS0 Padding</td>
</tr>
<tr>
<td></td>
<td>EDNS0 Keepalive</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Recursive resolver</th>
<th>Unbound</th>
<th>BIND</th>
<th>Knot Res</th>
</tr>
</thead>
</table>

- **Dark Green:** Latest stable release supports this
- **Light Green:** Patch available
- **Yellow:** Patch/work in progress, or requires building a patched dependency
- **Grey:** Not applicable or not yet planned

---

DNSOP@IETF96
Alternative server side solutions for TLS

• dnsdist would be great… but no support yet

• Pure TLS load balancer
  • NGINX, HAproxy,…
  • BIND article on using stunnel

But….
  • server must still have full TCP capabilities
  • pass through of edns-tcp-keepalive option
  • DNS specific access control is missing
# Stub implementations

<table>
<thead>
<tr>
<th>TCP/TLS Features</th>
<th>Idns (drill)</th>
<th>digit</th>
<th>getdns</th>
<th>BIND (dig)</th>
<th>Go DNS</th>
<th>Knot (kdig)</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP fast open</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connection reuse</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pipelining of queries</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Process OOOR</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EDNS0 Keepalive</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TLS Features</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TLS on port 853</td>
<td>Dark Green</td>
<td>Light Green</td>
<td>Yellow</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authentication of server</td>
<td>Light Green</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EDNS0 Padding</td>
<td></td>
<td>Light Green</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Dark Green**: Latest stable release supports this
- **Light Green**: Patch available
- **Yellow**: Patch/work in progress, or requires building a patched dependency
- **Grey**: Not applicable or not yet planned
DNS-over-TLS Deployment

- SERVERS: NLnet Labs and OARC offering experimental DNS-over-TLS servers:
  
  https://portal.sinodun.com/wiki/display/TDNS/DNS-over-TLS+test+servers

- CLIENT: getdns - 1.1.0a1 release of a DNS-over-TLS daemon mode - try it out:
  
  https://portal.sinodun.com/wiki/display/TDNS/DNS+Privacy+daemon
DNS-over-TLS services

• RIPE DNS WG: Presentation and discussion of offering experimental DNS Privacy Service

• RIPE are planning to co-ordinating a community effort
  • Research various solutions and issues
  • Output will be operational guidance
Ongoing Work

- Patches to dnsperf to do TCP/TLS performance benchmarking using RFC7766, etc.

- draft-ietf-dprive-dtls-and-tls-profiles-03

- 2 updates since IETF 95 - please review!