EDNS (in) Compatibility

Eddy Winstead, ISC
NANOG 65 - Montreal, Canada
October, 2015
What is EDNS?
Why would you want EDNS?

- DNSSEC, IPv6 (signature tool)
- Client-subnet Identifier (query)
- Client-subnet Identifier (identity query)
- DNSSEC, IPv6 (signature and/or several IPv6 originate)
- Client will be more new applications...
- DNS cookies (abuse mitigation tool)
1. Firewall blocking is indistinguishable from packet loss, causing DNS servers to retry uselessly, slowing response to users.

2. Poor failure modes can disable DNSSEC, making DNSSEC-signed sites unreachable for clients using validating resolvers.

3. New applications using EDNS may be stilled – DNS cookies (DDoS mitigation tool) – Client-subnet identifier (CDN optimization)

Why is EDNS compatibility a problem?
Firewalls may block the following:

- DNS queries with AD=1
- DNS queries with EDNS flag set
- Unknown EDNS options
- EDNS version not equal to 0
- DNS queries with EDNS flag set
- DNS queries with AD=1

These firewalls are not providing any ‘security’. All they are doing is stuffing up the ability to deploy protocol extensions. These firewalls are not providing any ‘security’ benefit to anyone by doing this. All they are doing is providing no ‘security’. Firewalls may block the following:
EDNS Compliance Tester

deterministic. we can see sooner rather than later as delaying will only increase the amount of timing re
That said we are testing all of the features of EDNS as we don't know when we are going
Cookies which require unknown EDNS options to be correctly handled by all servers.
ISC is testing EDNS Compliance because the lack of proper EDNS compliance impacts it

EDNS Compliance

Internet Systems Consortium

ednscomp.isc.org
<table>
<thead>
<tr>
<th></th>
<th>AU</th>
<th>GOV</th>
<th>Alexa Bottom</th>
<th>Alexa Top</th>
<th>TLD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full EDNS Aware Servers</td>
<td>96%</td>
<td>98%</td>
<td>92%</td>
<td>96%</td>
<td>100%</td>
</tr>
<tr>
<td>EDNS Awareness</td>
<td>96%</td>
<td>96%</td>
<td>61%</td>
<td>61%</td>
<td>80%</td>
</tr>
</tbody>
</table>


(Sept 15, 2015)
What can you do?

- Test your DNS services at ednscomp.isc.org
- Keep your DNS servers updated
- Keep in mind while debugging DNSSEC validation failures
- Remove rules blocking EDNS responses from Firewalls
- Test your DNS services at ednscomp.isc.org