EDNS (in) Compatibility

October, 2015

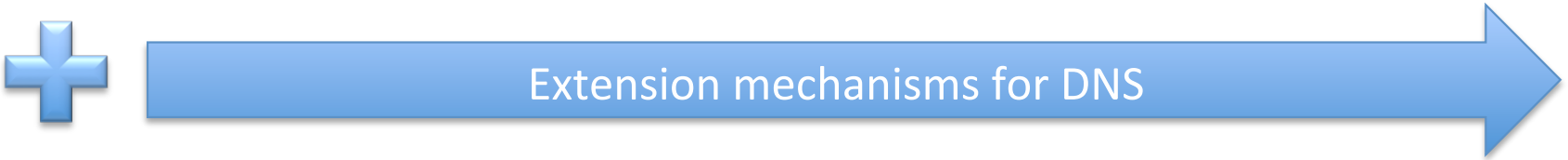
NANOG 65 - Montreal, Canada

Eddy Winstead, ISC

What is EDNS?

Original max allowable size of a DNS message over UDP

512 bytes



2000ish+ DNS msg max over UDP, up to 4096 bytes

512	512	512	512	512	512	512	512

Why would you want EDNS?

- DNSSEC, IPv6 (signatures and/or several IPv6 addresses)
- Client-subnet Identifier (identify query originator)
- DNS cookies (abuse mitigation tool)
- there will be more new applications ...

Why is EDNS compatibility a problem?

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 stifled
   - DNS cookies (DDOS mitigation tool)
   - Client-subnet identifier (CDN optimization)

Firewalls may block the following:

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

"These firewalls are not providing any 'security' benefit to anyone by doing this. All they are doing is stuffing up the ability to deploy protocol extensions."

ednscomp.isc.org

Internet Systems
Consortium

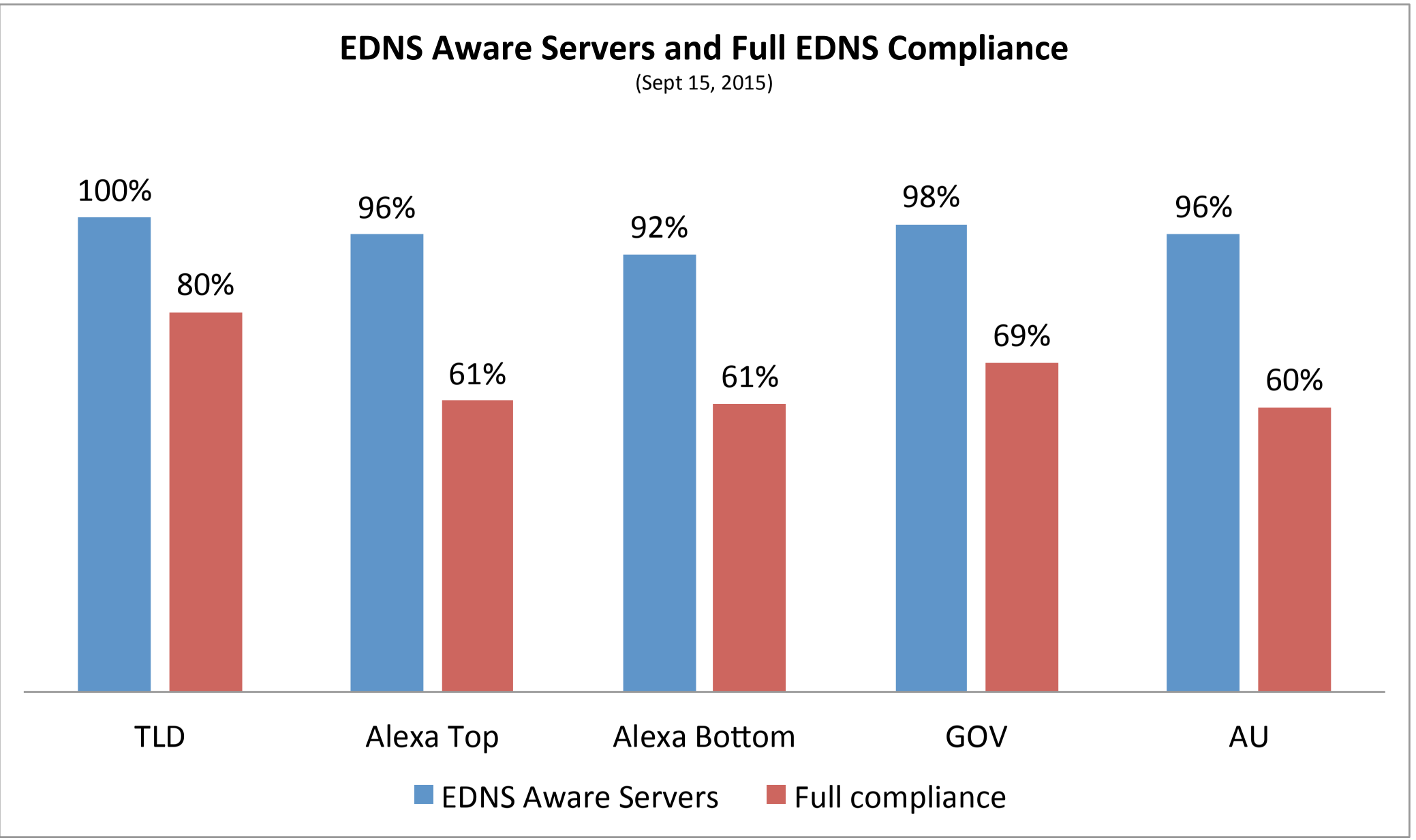
EDNS Compliance

ISC is testing EDNS compliance because the lack of proper EDNS compliance impacts tl
Cookies which requires Unknown EDNS Options to be correctly handled by all servers.

That said we are testing all of the features of EDNS as we don't know when we are going
we can see sooner rather than later as delaying will only increase the amount of fixing re
deterministic.

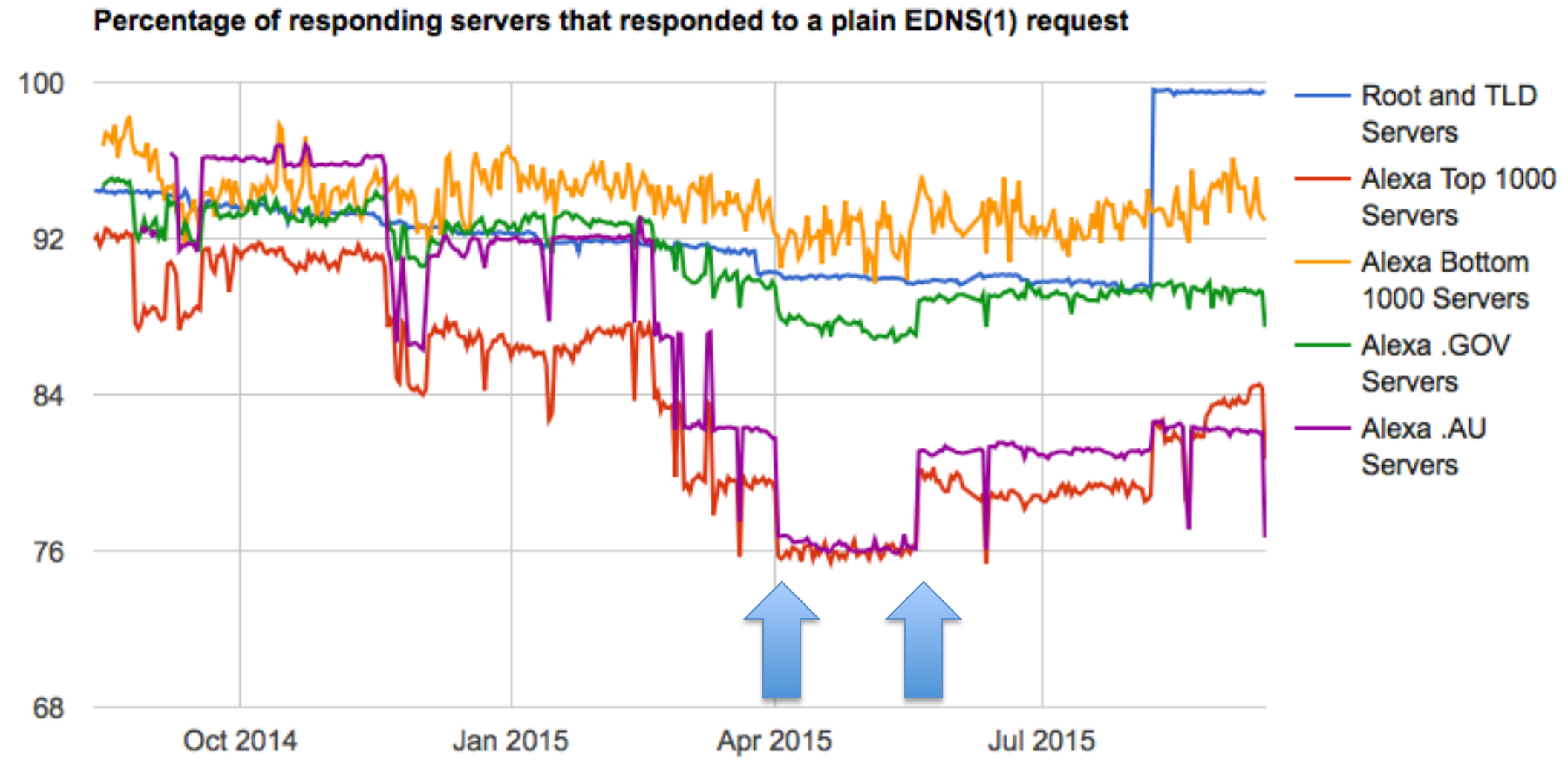
EDNS Compliance Tester

Test Your Servers Here



http://ednscomp.isc.org/compliance/summary.html

5-20 Route 53 Firewall updated



What can you do?

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