Test Report:
DNSSEC Impact on Broadband Routers and Firewalls
September, 2008

Ray Bellis
Nominet UK
ray.bellis@nominet.org.uk

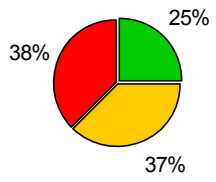
Lisa Phifer
Core Competence
lisa@corecom.com

Executive Summary

To assess potential impact of DNSSEC on broadband consumers, we tested two dozen residential Internet router and SOHO firewall devices commonly used with broadband services. In summary, we found that:

- All 24 units could **route** DNSSEC queries addressed to upstream resolvers (referred to herein as route mode) without size limitations.
- 22 units could **proxy** DNS queries addressed directly to them (referred to herein as proxy mode), with varying degrees of success.
- 6 of 22 DNS proxies had difficulty with DNSSEC-related flags and/or validated responses that effectively prevented DNSSEC use in proxy mode.
- 16 of 22 DNS proxies could successfully pass DNSSEC queries and return validated responses of some size.
- 18 DNS proxies limited responses over UDP to either 512 bytes or a size constrained by the MTU. Only 4 could return responses over UDP up to 4096 bytes, while just 1 could proxy DNS over TCP (no size limit). Such limits can interfere with returning longer DNSSEC responses.
- When deployed with factory defaults, 15 units are likely to be used as DNS proxies, while 3 always route DNS queries. The rest (6) vary over time, preferring to route DNS after being connected to a WAN.

As a consequence, we conclude that just 6 units (25%) operate with full DNSSEC compatibility "out of the box." 9 units (37%) can be reconfigured to bypass DNS proxy incompatibilities. Unfortunately, the rest (38%) lack reconfigurable DHCP DNS parameters, making it harder for LAN clients to bypass their interference with DNSSEC use.



These findings, their potential impact on DNSSEC use by broadband consumers, and implications for router/firewall manufacturers, are presented and analyzed in this report.

Table of Contents

1. Introduction

During July and August 2008, Core Competence and Nominet collaborated to develop and conduct a series of tests, intended to assess the impact of DNSSEC on residential Internet router and SOHO firewall devices commonly used with broadband services. This report documents our findings.

1.1 Objective

To assess router/firewall support for (or interference with) DNS queries pertaining to DNSSEC-signed domains, as well as DNSSEC queries on unsigned domains, we conducted lab tests to determine whether each unit correctly routes and/or proxies:

- DNS queries requiring TCP or EDNS0 to convey lengthy DNSSEC responses
- Non-DNSSEC queries on signed and unsigned domains
- Non-DNSSEC queries that set other DNSSEC-related request flags
- DNSSEC queries that request server-side validation
- DNSSEC queries that request no server-side validation

1.2 Background

We started with tests originally developed by .SE and documented in "DNSSEC Tests of Consumer Broadband Routers" (February 2008, http://iis.se/docs/Routertester_en.pdf). Based on lessons learned from earlier efforts, we refined our tests to decouple testing of related features, examine DNSSEC handling more rigorously, increase test repeatability, and improve result reliability.

The tests described in this report were executed in closed, controlled test beds to enable repeated, deterministic execution. Nominet tested units with xDSL WAN ports, while Core Competence tested units with 10/100 Ethernet WAN ports. Between us, we set out to test the broadband router/firewalls most commonly used today in the US and UK. To maximize coverage, we used published market research, broadband provider websites, and retail "best seller" lists to identify the most widely-deployed:

- Residential Internet routers supplied by broadband providers
- Residential Internet routers purchased by consumers
- Entry-level firewall appliances purchased by Small/Home Offices (SOHOs)

To minimize duplication, we generally avoided Ethernet and xDSL variations of the same product, retesting products previously tested by .SE, or testing more than two products from the same family.

1.3 Acknowledgements

Core Competence's participation in this study was supported by Shinkuro, Inc., The Internet Society, ICANN, and Afilias, Ltd. The results reported here are the work of Core Competence and Nominet UK, and do not necessarily reflect the views of the sponsors. In addition, the authors would like to thank Patrik Wallström, Joakim Åhlund, and Roy Arends for their assistance during test development.

2. Test Methodology

All DNS queries were executed twice. In the first pass queries were addressed to an upstream DNSSEC-aware recursive resolver to verify that DNS packets could be routed transparently. For the second pass queries were addressed directly to the unit under test to exercise router/firewall DNS proxies. These DNS usage styles are referred to throughout this report as **route mode** and **proxy mode**, respectively.

Nearly all upstream tests were successful; most of our findings pertain to problems with DNS proxy handling of DNSSEC queries and the lengthy responses they can generate. To determine where and how these problems occur, we examined the following cases.

2.1 Test Cases

T) TCP/IP Compatibility: Can the unit route or proxy DNS queries to a DNSSEC-aware resolver over TCP?

> DNSSEC responses may not fit into one 512-byte UDP packet. When UDP queries fail, clients may revert automatically to TCP. Where both TCP and EDNS0 are not supported, DNS queries on signed domains may fail. To avoid orthogonal fail-overs during later tests, we determined TCP and UDP support at test start. We then conducted all DNSSEC tests over UDP, with responses shorter than 512 bytes.

A) EDNS0 Compatibility: Can the unit route or proxy DNS queries to a DNSSEC-aware resolver over UDP using EDNS0?

> For units that do not proxy DNS queries over TCP, EDNS0 is required to handle lengthy DNSSEC responses. To assess EDNS0 support, we queried four unsigned domains over UDP, using five different EDNS0 buffer sizes (512, 1024, 1536, 2048, 4096 bytes). Queried domains return TXT records of increasing (but consistent and predictable) lengths, designed to fit in certain buffer sizes and be truncated at others. Results indicate whether the router/firewall can return lengthy responses using EDNS0 and limits imposed on UDP response size. For test independence, we did not permit truncated UDP tests to fail-over to TCP.

B) DNSSEC-Signed Domain Compatibility: Can the unit route or proxy non-DNSSEC queries on signed domains to a DNSSEC-aware resolver?

> We ran this baseline before all other DNSSEC flag tests to isolate and eliminate unrelated failures causes (e.g., inability to reach upstream resolver, responses larger than 512 bytes, basic NAT problems). Units that cannot successfully handle these non-DNSSEC queries are unlikely to handle any other query with DNSSEC flags set.

E) DNSSEC Request Flag Compatibility: Can the unit route or proxy non-DNSSEC queries that set Authentic Data (AD) and/or Checking Disabled (CD) flags?

> We then queried signed and unsigned domains to ensure that setting the AD flag and/or the CD flag in a non-DNSSEC query did not adversely impact tested units.

These flags are carried in queries but are currently only meaningful in conjunction with the DNSSEC OK flag. We tested all possible AD/CD request flag permutations to isolate any underlying flag-handling bugs before making DNSSEC OK queries. See Appendix B for tested AD/CD flag permutations and expected responses.

C) DNSSEC OK (DO) Compatibility: Can the unit route or proxy DNSSEC queries that request server-side validation by setting the DNSSEC OK (DO) flag?

We queried signed and unsigned domains to verify that server-validated DNSSEC responses were correctly returned to the client, without modification, and flags set correctly.

- Signed domain queries with DO=1 should return a complete DNSSEC response with AD=1, indicating that the response contains authenticated data.

- Unsigned domain queries with DO=1 should return a plain DNS response with AD=0, indicating that authenticated data was not available.

To pass this test, the router/firewall must pass the client's DO request flags to the security-aware server and do nothing to modify that server's response. Test zone TTLs were set to zero to prevent the resolver and/or proxy from returning previously-validated cached responses.

D) Checking Disabled (CD) Compatibility: Can the unit route or proxy DNSSEC queries that disable server validation by setting both DO and CD flags?

We queried signed and unsigned domains with Checking Disabled (CD=1) to ensure that non-validated DNSSEC responses were correctly returned to the client, without modification and with the expected flags set.

- Signed domain queries with both DO=1 and CD=1 should return a complete DNSSEC response with CD=1 and AD=0, indicating that validation was neither requested nor performed.

- Unsigned domain queries with both DO=1 and CD=1 should return a plain DNS response with CD=1 and AD=0, indicating that validation was neither requested nor performed.

Here again, to pass this test, the router/firewall must pass the client's CD request to the security-aware server and do nothing to modify that server's response.

F) Other DNS Security Tests: In addition to transport and DNSSEC flag tests, we took this opportunity to look for the following DNS router/firewall security issues:

No Open Resolver: Does the router/firewall ignore or explicitly reject DNS queries that originate from the Internet, sent to the unit's WAN port?

Source Port Randomization: Does the router/firewall NAT preserve inside DNS resolver source port randomization (e.g., to mitigate packet spoofing)?

0x20 Bit Support: Does the router/firewall preserve case distinctions in the domain names carried by DNS queries (e.g., to deter response forgery)?

All test commands, expected "success" responses, and common failure conditions are described in Appendix B. Test results are analyzed in Section 3.

2.2 Test Beds

Nominet and Core Competence test beds each contained DNS clients (BIND 9.5.0-P1 *dig*, *Net::DNS* 0.63, *NET::DNS::SEC* 0.14) and a pair of local DNSSEC-aware resolvers (two instances of BIND 9.5.0-P1 *named*, running on a single server). DNS clients and servers were connected to the router/firewall under test by 10/100 Ethernet or a DSLAM.

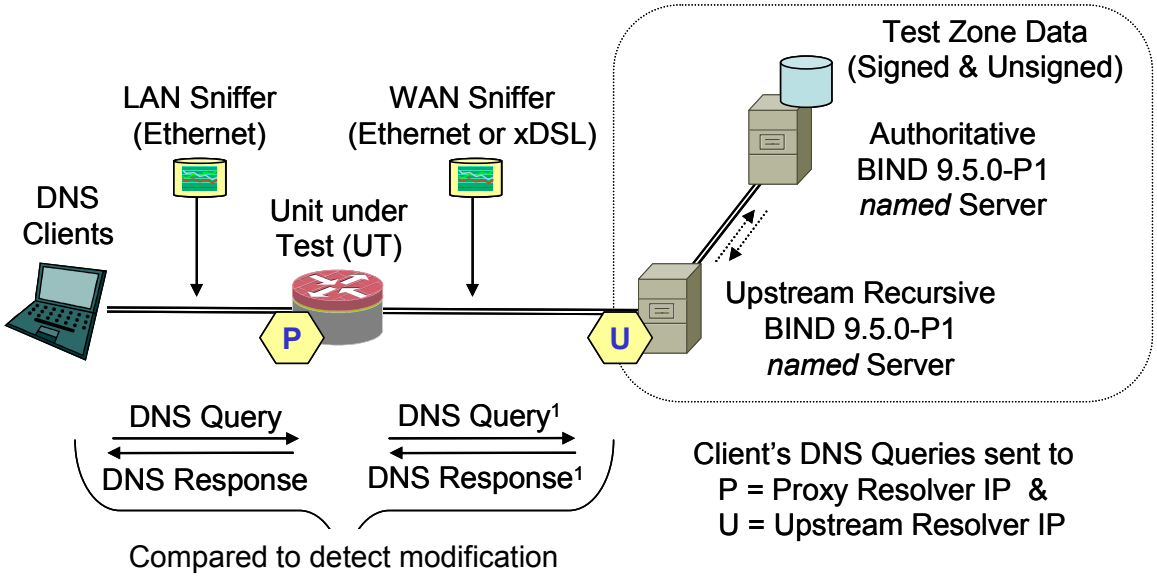


Figure 1. Test Environment

Earlier experiments showed that Internet-based tests could fail due to intermittent delays and outages. Repeatability was also affected by remote caching, software upgrades, and zone data updates. To avoid those problems, we created closed test beds; all systems consulted during our test runs were local.

Local authoritative resolvers in both test beds were populated with signed and unsigned records. Zone content and record lengths were chosen to avoid triggering EDNS0 and TCP failures during DNSSEC tests and exercise EDNS0 buffer sizes.

Each unit was tested in near-factory-default condition, with the minimum necessary changes required to set up the test scenario (e.g., enabling DHCP, setting the WAN DNS to the local recursive resolver). This is how most residential broadband subscribers actually deploy these routers and firewalls, and lets us assess the likely impact of DNSSEC on those consumers. Each unit was tested with the factory-shipped firmware. However, we also noted where firmware updates were available and retested all of those units at project end, finding just one difference that impacted test outcomes.

3. Test Results

Query responses were recorded at the DNS client and sniffers were used to capture DNS packets on both sides of the unit under test. Responses were compared to reference responses and defined success/failure criteria to determine test outcome.

3.1 Result Summary

Test outcomes are summarized in Table 2 below.

	Make/Model		Out of the Box Usage Mode	Route DNS to Upstream Resolver	Proxy DNS over UDP	A. EDNS0 Compatibility	B. Signed Domain Compatibility	E. Request Flag Compatibility	D. Checking Disabled Compatibility	C. DNSSEC OK Compatibility	Proxy DNS over TCP
			DHCP DNS	No Proxy	UDP Proxy Transport Tests		UDP Proxy DNSSEC Tests				TCP Proxy
1	2Wire	270HG-DHCP	Proxy	OK	OK	FAIL	OK	OK	FAIL	FAIL	FAIL
2	Actiontec	MI424-WR	Proxy	OK	OK	FAIL > 512	OK	OK	OK	OK	FAIL
3	Apple	Airport Express	Proxy	OK	OK	FAIL > 512	OK	FAIL	FAIL	FAIL	OK
4	Belkin	N (F5D8233)	Proxy	OK	OK	FAIL > 1500	OK	OK	OK	OK	FAIL
5	Belkin	N1 (F5D8631)	Proxy	OK	OK	FAIL > 1500	OK	OK	OK	OK	FAIL
6	Cisco	c871	Route	OK	OK	FAIL > 512	OK*	OK*	OK*	OK*	FAIL
7	D-Link	DI-604	Proxy	MIX	OK	FAIL > 1472	OK	OK	OK	OK	FAIL
8	D-Link	DIR-655	Proxy	OK	OK	OK	OK	OK	OK	OK	FAIL
9	Draytek	Vigor 2700	Proxy	OK	OK	FAIL > 1464	OK	FAIL	FAIL	OK	FAIL
10	Juniper	SSG-5	Route	OK	OK	OK	OK	OK	OK	OK	FAIL
11	Linksys	BEFSR41	Varies	OK	OK	FAIL > 1472	OK	OK	OK	OK	FAIL
12	Linksys	WAG200G	Varies	OK	OK	OK	OK	OK	OK	OK	FAIL
13	Linksys	WAG54GS	Varies	OK	OK	OK	OK	OK	OK	OK	FAIL
14	Linksys	WRT150N	Varies	OK	OK	FAIL > 512	OK	OK	OK	OK	FAIL
15	Linksys	WRT54G	Varies	OK	OK	FAIL > 512	OK	OK	OK	OK	FAIL
16	Netgear	DG834G	Proxy	OK	OK	FAIL > 512	OK	FAIL	FAIL	MIX	FAIL
17	Netopia	3387WG-VGx	Proxy	OK	OK	FAIL > 512	OK	FAIL	FAIL	FAIL	FAIL
18	SMC	WBR14-G2	Proxy	MIX	OK	FAIL > 512	OK	OK	OK	OK	FAIL
19	SonicWALL	TZ-150	Route	OK	n/a	n/a	n/a	n/a	n/a	n/a	n/a
20	Thomson	ST546	Proxy	OK	OK	FAIL > 512	OK	OK	OK	OK	FAIL
21	WatchGuard	Firebox X5w	Varies	OK	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL
22	Westell	327W	Proxy	OK	OK	FAIL	OK	OK	FAIL	FAIL	FAIL
23	ZyXEL	P660H-D1	Proxy	OK	OK	FAIL > 1464	OK	OK	OK	OK	FAIL
24	ZyXEL	P660RU-T1	Proxy	OK	OK	FAIL > 1464	OK	OK	OK	OK	FAIL

Table 2. Test Result Summary
(see Appendix A for further detail)

3.2 Result Analysis

We offer the following observations about the test outcomes shown in Table 2:

- All 24 units could **route** DNSSEC queries transparently to upstream resolvers without flag or length limitations.
- All 22 units with DNS **proxies** could handle non-DNSSEC queries about signed domains.
- 6 of 22 DNS proxies had difficulty with DNSSEC-related flags and/or validated responses that effectively prevented DNSSEC use in proxy mode.
- 16 of 22 DNS proxies could successfully pass DNSSEC queries and return validated responses of some length.
- 18 proxies limited DNS response size over UDP to either 512 bytes, or a total packet size constrained by the MTU.
- 4 proxies could return UDP/EDNS0 responses up to 4096 bytes.
- Just one unit could proxy DNS over TCP.
- When deployed with factory defaults, 15 units are likely to be used as DNS proxies, while 3 always route DNS queries. The rest (6) vary over time, routing DNS to an upstream resolver only after being connected to a WAN.
    - 6 units operate with full DNSSEC compatibility "out of the box."
    - 9 units can be reconfigured to bypass their DNS proxy incompatibilities.
    - 9 units lack reconfigurable DHCP DNS parameters, making it harder for LAN clients to bypass their DNSSEC incompatibilities.
- All units faithfully copied 0x20 bits; two were open resolvers.
- Half of these units did not preserve source port randomization.

These observations and their impact on DNSSEC usage are analyzed below.

"Out of the Box" DNS Usage

When LAN DHCP defaults are used to supply DNS server addresses to clients, most broadband router/firewalls identify themselves as the local DNS, while others supply the ISP's DNS address (usually inherited from WAN link settings). In this report, a unit that defaults to its own address is said to prefer DNS proxy mode, while a unit that defaults to an upstream resolver's address is said to prefer DNS route mode.

To avoid ambiguity or error, all DNS test queries were explicitly addressed to the router/firewall or upstream resolver. However, we also recorded LAN DHCP defaults (summarized in Table 2, see Appendix A for details) because they reflect how most broadband consumers use tested products, and therefore the potential impact of any DNSSEC issues.

			Target Environment	Out-of-the-Box Usage Mode	Configurable DHCP DNS	Routes DNSSEC (TCP and UDP)	Proxies DNSSEC (UDP Only)
1	2Wire	270HG-DHCP	Residential	Proxy	NO	YES	NO
2	Actiontec	MI424-WR	Residential	Proxy	NO	YES	MIX
3	Apple	Airport Express	Residential	Proxy	NO	YES	NO
4	Belkin	N (F5D8233)	Residential	Proxy	NO	YES	MIX
5	Belkin	N1 (F5D8631)	Residential	Proxy	NO	YES	MIX
6	Cisco	c871	SOHO	Route	YES	YES	MIX
7	D-Link	DI-604	Residential	Proxy	NO	MIX	MIX
8	D-Link	DIR-655	Residential	Proxy	YES	YES	YES
9	Draytek	Vigor 2700	Residential	Proxy	YES	YES	NO
10	Juniper	SSG-5	SOHO	Route	YES	YES	YES
11	Linksys	BEFSR41	Residential	Varies	YES	YES	MIX
12	Linksys	WAG200G	Residential	Varies	YES	YES	YES
13	Linksys	WAG54GS	Residential	Varies	YES	YES	YES
14	Linksys	WRT150N	Residential	Varies	YES	YES	MIX
15	Linksys	WRT54G	Residential	Varies	YES	YES	MIX
16	Netgear	DG834G	Residential	Proxy	YES	YES	NO
17	Netopia	3387WG-VGx	Residential	Proxy	YES	YES	NO
18	SMC	WBR14-G2	Residential	Proxy	NO	MIX	MIX
19	SonicWALL	TZ-150	SOHO	Route	YES	YES	NO
20	Thomson	ST546	Residential	Proxy	NO	YES	MIX
21	WatchGuard	Firebox X5w	SOHO	Varies	YES	YES	NO
22	Westell	327W	Residential	Proxy	NO	YES	NO
23	ZyXEL	P660H-D1	Residential	Proxy	YES	YES	MIX
24	ZyXEL	P660RU-T1	Residential	Proxy	YES	YES	MIX

Table 3. "Out of the Box" Usage Summary

We found that 3 products were likely to be used in route mode because they do not proxy at all or require explicit configuration to enable the DNS proxy.

Another 6 products preferred route mode, but are likely to be used in proxy mode at least part-time because LAN DHCP DNS settings vary based on WAN state:

- One unit defaulted to proxy mode on first install. It then stored the ISP's DNS address in NVRAM for all future use, independent of WAN state.

- Five units defaulted to proxy mode at boot, subsequently delivering the ISP's DNS address in all DHCP leases obtained once the WAN was up. Clients are thus likely to use these DNS proxies after each reboot, until their initial lease expires (roughly 1 to 2 days).

The remaining 15 units preferred DNS proxy mode. In fact, 9 of these units could not be reconfigured to disable the proxy or deliver upstream resolver addresses to LAN DHCP clients. See section 4.1 for consumer impacts and DNSSEC compatibility conclusions.

Route DNS to Upstream Resolver

When LAN clients send DNS queries directly to the ISP's DNS, the router/firewall should route them transparently to that upstream resolver. Packets are firewalled and NAT'ed, but DNS client/server interaction (including DNSSEC) should not be impeded.

One unit repeatedly experienced a possible memory leak when routing our longest response, while another intercepted and proxied queries addressed to upstream resolvers (fixed in newer firmware). These exceptions demonstrate that transparent routing should not be taken for granted. But as a rule, we found that router/firewalls can generally route DNSSEC queries to upstream resolvers transparently, without adverse impact.

The rest of our findings pertain to router/firewall DNS proxy operation – the usage mode experienced by most residential broadband consumers.

Proxy DNS over TCP

Until the introduction of EDNS0 (see below) the only way to receive a DNS response exceeding 512 bytes was to use TCP instead of UDP.

Typically a DNS client would issue its initial request with UDP. If the response was too large the server would send back a UDP response with the TC ("Truncation") bit set. The client would then automatically fallback to using TCP.

Additionally, certain DNS operations (particularly Zone Transfers – "AXFR") are only intended to operate over TCP.

Disappointingly, we found that support for TCP in broadband router/firewall DNS proxies is almost non-existent. Virtually all DNS responses are therefore proxied over UDP, and all of our DNSSEC tests were conducted over UDP only, reflecting the way that most broadband consumers would experience DNSSEC.

Proxy DNS over UDP - EDNS0 Compatibility

EDNS0 (RFC 2671) is a method by which DNS clients can indicate to servers that they are able to receive UDP packets that are larger than the original RFC1035 maximum of 512 bytes.

This capability is indicated by including an Options (OPT) Resource Record (RR) in the Additional Section of the DNS query. Using EDNS0, clients may specify their maximum receive buffer size for DNS responses. To pass this test, proxies must process the client's query and:

- Return valid responses that fit in the specified buffer without truncation, or
- Indicate truncation for responses that would exceed the specified buffer.

For example, tests that generate 400 or 800 byte responses whilst specifying a buffer size of 1024 bytes should return those records without error or truncation, while tests that would otherwise generate 1600 or 3200 byte responses should return truncated responses with TC=1 at that buffer size.

Although nearly every proxy we tested supported UDP queries, most had some degree of difficulty supporting EDNS0 (summarized in the following graphs, explained below, see Appendix A for further detail).

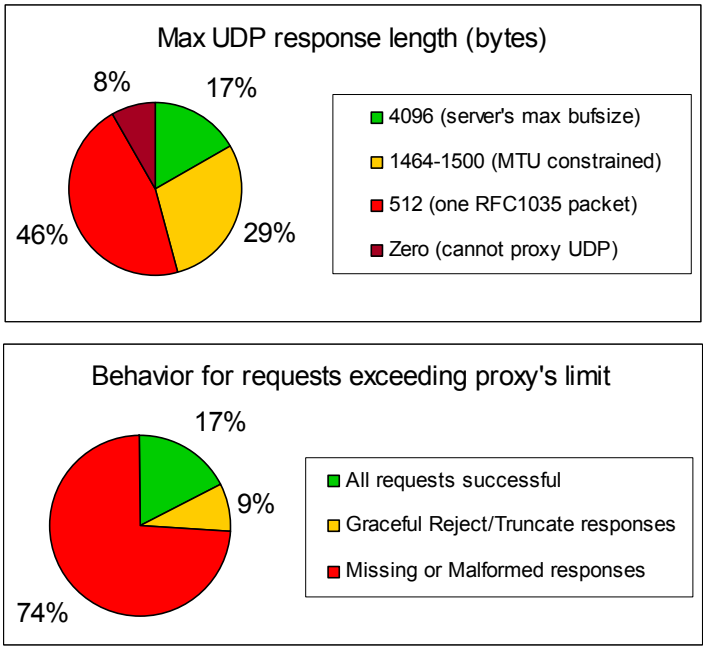


Figure 4. EDNS0 Compatibility

Various failure modes were noted:

- FORMERR response, indicating that the proxy does not support EDNS0.
- Correctly formed truncated response with TC=1, indicating that the proxy does not support the client's requested buffer size – this is standards compliant but still impacts DNSSEC compatibility (see Section 4).
- Malformed truncated response with TC=0, where only an initial portion of the upstream server's complete response is forwarded to the client.
- Malformed truncated response with TC=0, where the upstream server indicated truncation but the proxy cleared the flag.
- Upstream responses that exceed the proxy's internal limits are dropped, resulting in no proxy response, causing client timeouts.
- One or more fragments from responses exceeding the MTU are dropped, resulting in client fragment reassembly timeouts.
- Client requests that contain an OPT RR are dropped by the proxy without response, causing client timeouts.
- Fragments of the proxy's response coming from the wrong Source IP address, causing the client to ignore the fragment.

Where the proxy truncated the response, this was commonly either at 512 bytes (the original RFC 1035 specified maximum packet size) or at 28 bytes less than the WAN MTU (i.e. 1464 for ADSL routers and 1472 for most dual Ethernet routers/firewalls).

Based on these results, we find that most DNS proxies would be unable to return responses with a total packet size greater than the MTU size, while many could not return responses longer than 512 bytes.

Request Flag Compatibility

The CD ("Checking Disabled") flag is used to inform an upstream validating resolver that full DNSSEC validation is not required and that any DNSSEC-related resource records should be returned to the client. A security-aware resolver is expected to copy the CD bit from the request into its response (RFC4035, §3.2.2).

The "AD" ("Authentic Data") flag is currently only defined in DNS responses, to indicate that the upstream resolver has validated the signatures on the returned data. However, because of incomplete support for EDNS0, IETF work is in progress to define a query containing AD=1 to indicate that the client understands the AD bit and that the server may return the AD bit in responses. This response indicates that the server has validated the associated signatures, without returning those RRSIG RRs to the client. We found that this proposed change has already been implemented in ISC Bind 9.5.

In this test, we verify that the UDP proxy can pass client-specified AD/CD flags to the security-aware resolver without error, and then return the resolver's response without modification. Two primary failure modes were seen here:

- Two proxies simply dropped any DNS requests that had the AD or CD bit set. This may be due to a strict interpretation of the definition of the Z flags in §4.1.1 of RFC 1035 ("Reserved for future use. Must be zero in all queries and responses") without taking into account that future uses for these flags have now indeed been defined.
- One of those two also dropped any DNS response that had the AD bit set.
- Two proxies simply did not convey these flags from the client's DNS request to the upstream resolver, preventing correct interpretation and use.

In summary, we find that most proxies handled AD/CD request flags correctly. The handful that did not generally could not support any DNSSEC queries at all (see below).

DNSSEC OK Compatibility

RFC 3225 defined the DO ("DNSSEC OK") bit as a flag in the EDNS0 OPT RR that clients can use to indicate DNSSEC-awareness and request that the server return DNSSEC-related resource records. We ran two DO flag tests with and without the CD flag present.

The first two failure modes described above for EDNS0 effectively prevent the use of the DO flag as well. Unsurprisingly, therefore, the 6 proxies that failed the EDNS0 tests due to complete lack of support for the EDNS0 OPT RR also failed to handle any DNSSEC queries. Either plain RRs are returned without any indication of error, the query is explicitly rejected, or the query times-out.

One further failure mode was noted, where a proxy correctly forwarded the OPT RR to the upstream resolver, but then dropped any response containing authentic data (AD=1). This proxy also failed all of the AD/CD request tests, so appears to filter both requests and responses with the AD bit set.

In summary, 16 of 22 proxies – approximately 73% -- were capable of passing DNSSEC requests to a security-aware resolver and returning complete responses containing authentic data. The rest could not because they simply did not support the OPT RR needed to indicate DNSSEC-awareness.

Source Port Randomization

This test exercises the underlying Network Address Translation/Port Translation (NAT-PT) algorithms in the router/firewall.

We added this to our test methodology in light of the DNS vulnerability announced by Dan Kaminsky on July 8th 2008 and subsequent concerns that NAT-PT systems could undermine any source port randomization used by DNS servers located behind (inside) the router/firewall.

We tested for UDP source port randomization by running a local recursive DNS resolver on the LAN side of the unit under test, and then running the public port checker tests available at http://www.doxpara.com and https://www.dns-oarc.net/oarc/services/porttest

Half of the units tested have poor source port selection algorithms, with most of those picking sequential UDP source ports.

Because this is a security vulnerability that could potentially be exploited (rather than an EDNS0 or DNSSEC support issue) we will not disclose here which units are affected until the vendors have had an opportunity to resolve those (e.g. via firmware updates).

However, our findings demonstrate that broadband consumers should be encouraged to update factory-default firmware as vendors fix this highly-publicized vulnerability. Doing so could lead consumers to install upgrades that improve DNSSEC support as well.

3.3 General Observations

No router/firewall passed every single test. Several (6) did, however, pass every test apart from the TCP test. Such products facilitate DNSSEC deployment by avoiding adverse impact on broadband consumers.

One firewall was essentially transparent to DNSSEC because it does not proxy DNS at all. Only those units that proxy DNS or inspect application layer content are likely to interfere with DNSSEC processing in any way.

All tested proxies appear to be DNS forwarders. However, we found that "simple" proxies were less likely to impede DNSSEC interaction between clients and upstream security-aware resolvers. Proxies that blindly copied AD/CD/DO flags fared well in our DNSSEC tests, while proxies that actively participated in DNS application processing were more impacted by DNSSEC. Specifically:

- One proxy that operated as a caching forwarder cached all SOA records returned by test queries, irrespective of zone TTL. That proxy incorrectly served later DNSSEC queries from its cache, returning the SOA but not associated RRSIGs. We circumvented this by querying TXT records instead of SOAs.

- Another proxy that operated as a caching forwarder generated UDP queries and then failed over to TCP queries for every response over 512 bytes – no matter which protocol the client used. As a result, retrieving a lengthy DNSSEC domain required twice as many queries (UDP failure, followed by TCP) and the client had no way to avoid this.

- One firewall failed every proxy test because it put the upstream resolver's IP address on all response packets forwarded through the proxy! Because most clients reject DNS responses received from unexpected sources (see RFC 2181), this unit's otherwise error-free DNSSEC support was a moot point.

As expected, we found more feature diversity in SOHO firewalls than residential routers. In fact, our SOHO firewall sample size is really too small to draw broad conclusions about SOHO products. Nonetheless, we offer these observations:

- Most tested SOHO firewalls required explicit configuration of DHCP and DNS settings and did not operate in proxy mode by default. Because these products routed DNSSEC to upstream resolvers by default, fewer consumers are likely to be impacted by SOHO firewall *proxy* support or non-support of DNSSEC.

- A growing number of SOHO firewalls now provide deep packet inspection and/or application layer proxies, typically packaged as "unified threat management" options. We tested two SOHO firewalls with and without these UTM options enabled. Neither objected to DNSSEC flags or RRs used in our test queries and responses, although one did generate "possible reconnaissance" alerts. Further testing would be needed to assess this potential impact.

As described in Section 2.2, we used commands that were based on earlier .SE testing, refined to make it easier to determine which capability (or lack thereof) caused a given test to fail. As such, our results are not directly comparable to .SE test results. However, we can offer some general comparisons:

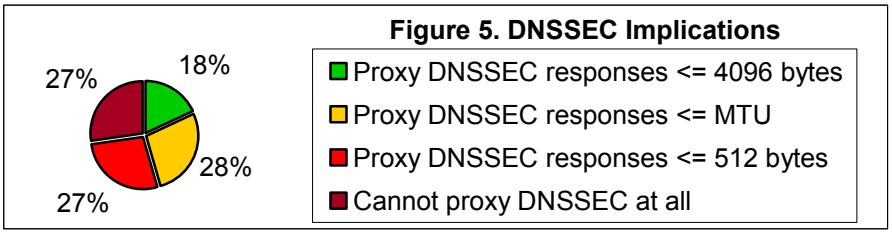
- Like .SE, we found near total absence of TCP and many EDNS0 limitations.
- We also found that 27% of proxies could not convey the DNSSEC OK flag.
- However, only two tested proxies blocked requests containing the AD flag.
- We did not experience as many failure results because we did not run as many tests over TCP or over UDP with expected responses > 512 bytes.

4. Conclusions

All 24 units could successfully route DNSSEC queries addressed directly to an upstream resolver. DNS clients could send DNSSEC queries and receive signed responses of any length when units were reconfigured to operate in this fashion.

However, most units operate as DNS proxies by default, almost always over UDP. This is how most broadband consumers will experience DNSSEC. When we combine our DNSSEC results with UDP/EDNS0 results for the 22 units that successfully proxy DNS (i.e., passed our baseline test), we find that:

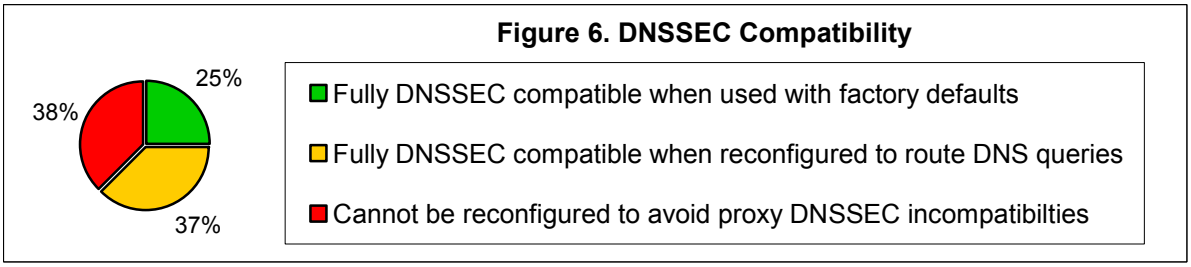
- 4 proxies could retrieve DNSSEC-enabled responses up to 4096 bytes (the max buffer size implemented by most servers, including ISC BIND)
- 6 proxies could only retrieve DNSSEC responses that fit in one IP packet
- 6 proxies could only retrieve DNSSEC responses that fit in one RFC1035 packet
- 6 proxies blocked "DNSSEC OK" requests and/or validated responses entirely



This is how we conclude that 16 of 22 DNS proxies – roughly 73% – can successfully pass DNSSEC queries and return validated responses of some size.

4.1 Consumer Impacts and Mitigation Strategies

None of the router/firewalls that we tested failed when a signed domain was queried without requesting DNSSEC resource records. This suggests that *domain signing* will have no impact on broadband consumers that *do not use* DNSSEC.



As illustrated above, 6 of the products we tested were fully compatible with DNSSEC using factory-default configurations. Here we include products that operated in their preferred mode(s) without any adverse impact on DNSSEC usage. This includes route mode units that passed all routed DNS tests, proxy mode units that passed all UDP-proxied DNS tests, and units that varied their usage mode but passed these tests in both modes.

18 other products proxied DNS using factory-default configurations and experienced at least some difficulty with DNSSEC flags, response size limits, or both. In these cases, DNS proxy limitations impact "out of the box" DNSSEC usage.

Fortunately, half (9) of those have configurable WAN and/or LAN DNS settings that could be used to instruct DHCP clients to address queries directly to an upstream resolver. When reconfigured in this manner, any DNS proxy limitations that impact DNSSEC usage would be bypassed. We therefore consider these products to be compatible with DNSSEC when reconfigured to use route mode.

However, the remaining 9 broadband routers offered no way to disable the DNS proxy or change LAN DNS settings, meaning that DHCP clients always address queries to the router. In these units, any DNS proxy incompatibilities will impact DNSSEC usage unless the clients (not the router) are reconfigured to hard-coded upstream resolver addresses. (Note that it is not impossible to use these products with DNSSEC -- just difficult.)

NB: Whilst hard-coding any DNS settings is undesirable, using DHCP to propagate DNS settings configured in the unit's DHCP server is preferable to hard-coding upstream DNS IPs into clients. Using DHCP for all client configuration requirements avoids the need to reconfigure mobile client devices used in different locations. Similarly, where a SOHO network contains many client devices, using a DHCP server (on the router or elsewhere on the local LAN) avoids having to hard-coded DNS settings on each client.

For router/firewalls that drop or reject DNSSEC OK (OPT RR) requests entirely, sending DNS queries to an upstream resolver is for now the only viable work-around to use DNSSEC. However, IETF AD request flag redefinition may permit some DNSSEC use even without OPT RR support in the future.

For router/firewalls that support DNSSEC OK to retrieve signed responses up to a size limit, consumers must be aware of their own product's limit and apply configuration work-arounds if/when DNSSEC responses are truncated. Consumers must also be aware of products that truncate without client notification (i.e., setting the TC bit.)

Finally, as vendors apply DNSSEC and other DNS security fixes (e.g., source port randomization), consumers should be encouraged to upgrade to the latest firmware. When we repeated our tests with the latest firmware for all units, just one product exhibited DNS improvements that would have altered test outcome.

4.2 Recommendations for Manufacturers

Based on our test results, we offer the following recommendations to manufacturers of broadband router/firewall products that wish to facilitate DNS security in general and DNSSEC in particular.

Let clients ask for DNSSEC: For the handful of proxies that are still not compatible with the EDNS0 OPT RR, avoid further implementation delay. As our tests demonstrated, the OPT RR is required to carry the DNSSEC OK flag, so any proxy that is incompatible with EDNS0 is also incompatible with DNSSEC.

Follow the Robustness Principle: Proxies should never silently drop packets containing “unexpected” flags. Pass those DNSSEC requests along to the upstream resolver, and let security-aware resolvers validate and reply to those requests.

Don't get in the way: Proxies that do more than simply forward DNS client queries – that is, proxies that operate as caching and/or recursive resolvers – will need to become security-aware to avoid becoming an impediment to DNSSEC deployment. Manufacturers can facilitate DNS proxy bypass by supporting LAN DHCP DNS reconfiguration.

Don't drop/truncate without notice: Proxies with limited support for EDNS0 can improve DNSSEC compatibility as follows:

- If blindly passing client requests on to upstream resolvers, ensure that the upstream resolver's whole reply is returned to the client (including all fragments), sourced from the proxy's IP address.
- If unable to return the whole reply, ensure correct client behavior by setting the TC bit to indicate truncation beyond the proxy’s internal limit (e.g., 512 bytes or MTU size).
- If refusing to proxy a request due to a perceived malformed packet, return a FORMERR response to the client rather than silently dropping the request.

Increase UDP response size: Many proxies that are already compatible with EDNS0 may still improve support for lengthy DNSSEC responses by correctly handling longer UDP packets and IP fragment reassembly.

Let clients fail over to TCP when UDP isn't enough: Even when all parties are fully compatible with EDNS0, most servers will not return responses longer than 4096 bytes over UDP. Adding the ability to proxy DNS over TCP would let clients fail over when UDP is just not enough. And don't proxy client TCP queries over UDP – trust clients to know when TCP is really necessary.

Strengthen overall DNS security: Although our focus was assessing DNSSEC impact, there are other router/firewall updates that could strengthen overall DNS security. Specifically, we find it encouraging that most vendors have already eliminated open WAN resolver vulnerabilities. We further recommend rapid implementation of NAT-PT algorithms that randomize source port selection to deter packet spoofing attacks – not just against DNS, but against any NAT'ed application.

Manufacturers and other DNS implementors who would like to discuss these recommendations and individual test results are invited to contact Ray Bellis (ray.bellis@nominet.org.uk).

Appendix A. Test Result Detail

For per-unit test details, visit http://download.nominet.org.uk/dnssec-cpe/DNSSEC-CPE-Detailed-Results.xls

Table 7. Test Result Details – Page 1 of 3

Manufacturer	**2Wire**	**Actiontec**	**Apple**	**Belkin**	**Belkin**	**Cisco**	**D-Link**	**D-Link**
Model	270HG-DHCP	MI424-WR	Airport Express	N (F5D8233)	N1 (F5D8631)	C871	DI-604	DIR-655
Hardware Version		C	A1264	4v3(01)	3	K9 V04	E1	A3
Firmware Version(s)	5.29.47-WIMAX	4.0.16.1.56.0.10.7	7.3.1	3.01.10	3.01.04	12.4(15)T4	3.20	1.10
	(current)	(current)	7.3.2	3.01.17		12.4(20)T	3.53	1.11
Default WAN Config Mode	DHCP	DHCP	DHCP	DHCP	PPPoA	Manual	DHCP	DHCP
Default LAN DHCP Setting	On	On	On	On	On	On	On	On
Default LAN DHCP Lease	1 day	1 day	4 hours	Infinite	Infinite	2 hours or 1 day	1 week	1 day
Default DHCP DNS (WAN down)	Self	Self	Self	Self	Self	None	Self	Self
Default DHCP DNS (WAN up)	Self	Self	Self	Self	Self	Upstream	Self	Self
"Out of the Box" DNS Usage	Proxy	Proxy	Proxy	Proxy	Proxy	**Route**	Proxy	Proxy
Reconfigurable **DHCP** DNS?	**No**	**No**	**No**	**No**	**No**	Yes	**No**	Yes
Default F/W	On	On	On	On	On	On	On	On
WAN Open Resolver?	No	No	No	No	No	No	No	No
WAN responds to ICMP Echo?	**Yes**	**Yes**	**Yes**	No	No	No	**Yes**	No
0x20 Bit Support	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DNSSEC Test Results								
Routes Queries sent to Upstream?	Yes	Yes	Yes	Yes	Yes	Yes	**MIX***	Yes
> T.TCP Support	OK	OK	OK	OK	OK	OK	**MIX***	OK
> T.UDP Support	OK	OK	OK	OK	OK	OK	**MIX***	OK
> A.x EDNS0 Support	OK	OK	OK	OK	OK	OK	OK	OK
> B.x Baseline Queries	OK	OK	OK	OK	OK	OK	OK	OK
> E.x Request Flag Handling	OK	OK	OK	OK	OK	OK	OK	OK
> D.x Checking Disabled Queries	OK	OK	OK	OK	OK	OK	OK	OK
> C.x DNSSEC OK Queries	OK	OK	OK	OK	OK	OK	OK	OK
Proxies Queries sent to Unit?	Yes	Yes	Yes	Yes	Yes	**If Configured**	Yes	Yes
# T.TCP Support	**FAIL**	**FAIL**	OK	**FAIL**	**FAIL**	**FAIL**	**FAIL**	**FAIL**
# T.UDP Support	OK	OK	OK	OK	OK	OK	OK	OK
# A.x EDNS0 Support	**FAIL**	**FAIL (>512)**	**FAIL (>512)**	**FAIL (>1500)**	**FAIL (>1500)**	**FAIL (>512)**	**FAIL (>1472)**	OK
# B.x Baseline Queries	OK	OK	OK	OK	OK	OK*	OK	OK
# E.x Request Flag Handling	OK	OK	**FAIL**	OK	OK	OK*	OK	OK
# D.x Checking Disabled Queries	**FAIL**	OK	**FAIL**	OK	OK	OK*	OK	OK
# C.x DNSSEC OK Queries	**FAIL**	OK	**FAIL**	OK	OK	OK*	OK	OK
						* If querying TXT not SOA	* Destinations Limited In 3.20	

Table 7. Test Result Details – Page 2 of 3

Manufacturer	**Draytek**	**Juniper**	**Linksys**	**Linksys**	**Linksys**	**Linksys**	**Linksys**	**Netgear**
Model	Vigor 2700	SSG-5	BEFSR41	WAG200G	WAG54GS	WRT150N	WRT54G	DG834G
Hardware Version		710(0)	4.3	1.0	1.0	1.1	3.1	v4
Firmware Version(s)	2.7.3.3_131701	5.4.0r3a.0	2.00.02	1.01.01	1.00.06	1.0.1.9	4.21.1	V5.01.01
	2.8.2	6.1.0r3	(current)	1.01.06		(current)	(current)	V5.01.09
Default WAN Config Mode	PPPoA	Manual	DHCP	PPPoA	PPPoA	DHCP	DHCP	PPPoA
Default LAN DHCP Setting	On	On	On	On	On	On	On	On
Default LAN DHCP Lease	3 days	1 min or 3 days	1-2 days	1 day	1 day	1-2 days	1-2 days	3 daus
Default DHCP DNS (WAN down)	Self	192.168.2.254	Self*	Self*	Self*	Self*	Self*	Self
Default DHCP DNS (WAN up)	Self	Upstream	Upstream	Upstream	Upstream	Upstream	Upstream	Self
"Out of the Box" DNS Usage	Proxy	**Route**	**Varies**	**Varies**	**Varies**	**Varies**	**Varies**	Proxy
Reconfigurable **DHCP** DNS?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Default F/W	Off	On	On	On	On	On	On	On
WAN Open Resolver?	No	No	No	No	No	No	No	No
WAN responds to ICMP Echo?	No	No	No	No	No	No	No	No
0x20 Bit Support	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DNSSEC Test Results								
Routes Queries sent to Upstream?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
> T.TCP Support	OK	OK	OK	OK	OK	OK	OK	OK
> T.UDP Support	OK	OK	OK	OK	OK	OK	OK	OK
> A.x EDNS0 Support	OK	OK	OK	OK	OK	OK	OK	OK
> B.x Baseline Queries	OK	OK	OK	OK	OK	OK	OK	OK
> E.x Request Flag Handling	OK	OK	OK	OK	OK	OK	OK	OK
> D.x Checking Disabled Queries	OK	OK	OK	OK	OK	OK	OK	OK
> C.x DNSSEC OK Queries	OK	OK	OK	OK	OK	OK	OK	OK
Proxies Queries sent to Unit?	Yes	**If Configured**	Yes	Yes	Yes	Yes	Yes	Yes
# T.TCP Support	**FAIL**	**FAIL**	**FAIL**	**FAIL**	**FAIL**	**FAIL**	**FAIL**	**FAIL**
# T.UDP Support	OK	OK	OK	OK	OK	OK	OK	OK
# A.x EDNS0 Support	**FAIL (>1464)**	OK	**FAIL (>1472)**	OK	OK	**FAIL (>512)**	**FAIL (>512)**	**FAIL (>512)**
# B.x Baseline Queries	OK	OK	OK	OK	OK	OK	OK	OK
# E.x Request Flag Handling	**FAIL**	OK	OK	OK	OK	OK	OK	**FAIL**
# D.x Checking Disabled Queries	**FAIL**	OK	OK	OK	OK	OK	OK	**FAIL**
# C.x DNSSEC OK Queries	OK	OK	OK	OK	OK	OK	OK	**MIX***
			* WAN usually up **before** DHCP	* WAN usually up **after** DHCP	* WAN usually up **after** DHCP	* WAN / DHCP order varies	* WAN usually up **before** DHCP	* C.D0.U OK

Table 7. Test Result Details – Page 3 of 3

Manufacturer	**Netopia**	**SMC**	**SonicWALL**	**Thomson**	**WatchGuard**	**Westell**	**Zyxel**	**Zyxel**
Model	3387WG-VGx	WBR14-G2	TZ-150	ST546	Firebox X5w	327W	P660H-D1	P660RU-T1
Hardware Version	-	01 PN 752.8607	Rev.A	v6	ROM 7.2.1	D90-W11-06		2
Firmware Version(s)	7.7.4r4 (current)	1.05 1.08	3.1.0.15-95s 3.1.5.0	6.2.17.5	FW 7.5.2 (current)	4.0.3.02.02 (current)	V3.40(AGD.2)	V3.40(BGA.0)
Default WAN Config Mode	DHCP	DHCP	Manual	PPPoA	Manual	PPPoA	PPPoA	PPPoA
Default LAN DHCP Setting	On	On	On	On	On	On	On	On
Default LAN DHCP Lease	1 min or 1 hour	1 day	1 day	1 day	1 day	1 day	3-9 days	3-9 days
Default DHCP DNS (WAN down)	Self	Self	None	Self	Self*	Self	Self	Self
Default DHCP DNS (WAN up)	Self	Self	Upstream	Self	Upstream	Self	Self	Self
"Out of the Box" DNS Usage	Proxy	Proxy	**Route**	Proxy	**Varies**	Proxy	Proxy	Proxy
Reconfigurable **DHCP** DNS?	Yes	**No**	Yes	**No**	Yes	**No**	Yes	Yes
Default F/W	Off	Off	On	On	On	On	On	n/a
WAN Open Resolver?	No	**Yes**	No	No	No	No	No	**Yes**
WAN responds to ICMP Echo?	**Yes**	**Yes**	No	No	No	No	No	**Yes**
0x20 Bit Support	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DNSSEC Test Results								
Routes Queries sent to Upstream?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
> T.TCP Support	OK	OK	OK	OK	OK	OK	OK	OK
> T.UDP Support	OK	OK	OK	OK	OK	OK	OK	OK
> A.x EDNS0 Support	OK	**MIX***	OK	OK	OK	OK	OK	OK
> B.x Baseline Queries	OK	OK	OK	OK	OK	OK	OK	OK
> E.x Request Flag Handling	OK	OK	OK	OK	OK	OK	OK	OK
> D.x Checking Disabled Queries	OK	OK	OK	OK	OK	OK	OK	OK
> C.x DNSSEC OK Queries	OK	OK	OK	OK	OK	OK	OK	OK
Proxies Queries sent to Unit?	Yes	Yes	**No**	Yes	Yes	Yes	Yes	Yes
# T.TCP Support	**FAIL**	**FAIL**	n/a	**FAIL**	**FAIL**	**FAIL**	**FAIL**	**FAIL**
# T.UDP Support	OK	OK	n/a	OK	**FAIL**	OK	OK	OK
# A.x EDNS0 Support	**FAIL (>512)**	**FAIL (>512)**	n/a	**FAIL (>512)**	**FAIL**	**FAIL**	**FAIL (>1464)**	**FAIL (>1464)**
# B.x Baseline Queries	OK	OK	n/a	OK	**FAIL**	OK	OK	OK
# E.x Request Flag Handling	**FAIL**	OK	n/a	OK	**FAIL**	OK	OK	OK
# D.x Checking Disabled Queries	**FAIL**	OK	n/a	OK	**FAIL**	**FAIL**	OK	OK
# C.x DNSSEC OK Queries	**FAIL**	OK	n/a	OK	**FAIL**	**FAIL**	OK	OK
		* Intermittent Timeout @ 4096			* First use only, Upstream after			

Table 8. EDNS0 Test Detail Summary

Make and Model	Client Bufsize	512 bytes					1024 bytes					1536 bytes					2048 bytes					4096 bytes					Max DNS UDP Rsp
	Expected Rsp	400	TC	TC	TC	TC	400	800	TC	TC	TC	400	800	TC	TC	TC	400	800	1600	TC	TC	400	800	1600	2400	3200	
2Wire	270HG-DHCP	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	512
Actiontec	MI424-WR	0	0	0	0	0	0	3	0	0	0	0	3	0	0	0	0	3	3	0	0	0	3	3	3	3	512
Apple	Airport Express	0	0	0	0	0	0	2	0	0	0	0	2	0	0	0	0	2	2	0	0	0	2	2	2	2	512
Belkin	N F5D8233	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	0	0	0	0	4	4	4	1500
Belkin	N1 F5D8631	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	0	0	0	0	4	4	4	1500
Cisco	C871	0	0	0	0	0	0	3	0	0	0	0	3	0	0	0	0	3	3	0	0	0	3	3	3	3	512
D-Link	DI-604	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	0	0	0	0	4	4	4	1472
D-Link	DIR-655	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4096
Draytek	Vigor 2700	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	0	0	0	0	4	4	4	1464
Juniper	SSG-5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4096
Linksys	BEFSR41	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	0	0	0	0	4	4	4	1472
Linksys	WAG200G	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4096
Linksys	WAG54GS	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4096
Linksys	WRT150N	0	3	3	3	3	0	3	3	3	3	0	3	3	3	3	0	3	3	3	3	0	3	3	3	3	512
Linksys	WRT54G	0	3	3	3	3	0	3	3	3	3	0	3	3	3	3	0	3	3	3	3	0	3	3	3	3	512
Netgear	DG834G	0	0	0	0	0	0	3	0	0	0	0	3	0	0	0	0	3	3	0	0	0	3	3	3	3	512
Netopia	3387WG-VGx	0	3	3	3	3	0	3	3	3	3	0	3	3	3	3	0	3	3	3	3	0	3	3	3	3	512
SMC	WBR14-G2	0	0	0	0	0	0	4	0	0	0	0	4	0	0	0	0	4	4	0	0	0	4	4	4	4	512
SonicWALL	TZ-150	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0
Thomson	ST546	0	0	0	0	0	0	3	0	0	0	0	3	0	0	0	0	3	3	0	0	0	3	3	3	3	512
WatchGuard	Firebox X5w	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	0
Westell	327W	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	512
Zyxel	P660H-D1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	0	0	0	0	3	3	3	1464
Zyxel	P660RU-T1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	0	0	0	0	3	3	3	1464

Severity	Behavior
0	Responds with complete, valid rsp (TXT <= Bufsize)
0	Responds with TC=1 when expected (TXT > Bufsize)
1	Rejects EDNS0 with FORMERR
2	Responds with TC=1 when unexpected (TXT <= Bufsize)
3	Returns malformed truncated response with TC=0
4	Returns no response (includes incomplete fragments)
4	Returns reponse from unexpected source
	N/A (does not proxy DNS over TCP)

Appendix B. Test Commands

Actual test queries are described below using BIND dig syntax, along with expected "success" results. However, implementing these tests with dig is not required – it is only necessary to send the same DNS queries and look for the same DNS responses.

All test queries are explicitly sent to three IP addresses:

@UPSTREAM	Upstream Resolver (BIND Server's IP)	Tests T,A,B,C,D,E
@PROXY	Proxy Resolver (Router's LAN IP)	Tests T,A,B,C,D,E
@WAN	WAN Resolver (Router's WAN IP)	Test F Only

Test Num	Dig Command			Success
	TCP/IP Compatibility			
T.TCP	dig @<IP> +retry=0 +qr +tcp s.txt TXT			Rsp:TXT
T.UDP	dig @<IP> +retry=0 +qr +notcp s.txt TXT			Rsp:TXT
T.VER	dig @<IP> +retry=0 +qr +notcp version.bind CH TXT			Rsp:Version
	EDNS0 Compatibility			
A.512.S	dig @<IP> +retry=0 +qr +bufsize=512 +edns=0 +ignore s.txt TXT			Rsp:400 bytes
A.512.M	dig @<IP> +retry=0 +qr +bufsize=512 +edns=0 +ignore m.txt. TXT			Err:TC=1 ***
A.512.L	dig @<IP> +retry=0 +qr +bufsize=512 +edns=0 +ignore l.txt TXT			Err:TC=1
A.512.XL	dig @<IP> +retry=0 +qr +bufsize=512 +edns=0 +ignore xl.txt TXT			Err:TC=1
A.512.XXL	dig @<IP> +retry=0 +qr +bufsize=512 +edns=0 +ignore xxl.txt TXT			Err:TC=1
A.1024.S	dig @<IP> +retry=0 +qr +bufsize=1024 +edns=0 +ignore s.txt TXT			Rsp:400 bytes
A.1024.M	dig @<IP> +retry=0 +qr +bufsize=1024 +edns=0 +ignore m.txt TXT			Rsp:800 bytes
A.1024.L	dig @<IP> +retry=0 +qr +bufsize=1024 +edns=0 +ignore l.txt TXT			Err:TC=1
A.1024.XL	dig @<IP> +retry=0 +qr +bufsize=1024 +edns=0 +ignore xl.txt TXT			Err:TC=1
A.1024.XXL	dig @<IP> +retry=0 +qr +bufsize=1024 +edns=0 +ignore xxl.txt TXT			Err:TC=1
A.1536.S	dig @<IP> +retry=0 +qr +bufsize=1536 +edns=0 +ignore s.txt TXT			Rsp:400 bytes
A.1536.M	dig @<IP> +retry=0 +qr +bufsize=1536 +edns=0 +ignore m.txt TXT			Rsp:800 bytes
A.1536.L	dig @<IP> +retry=0 +qr +bufsize=1536 +edns=0 +ignore l.txt TXT			Err:TC=1
A.1536.XL	dig @<IP> +retry=0 +qr +bufsize=1536 +edns=0 +ignore xl.txt TXT			Err:TC=1
A.1536.XXL	dig @<IP> +retry=0 +qr +bufsize=1536 +edns=0 +ignore xxl.txt TXT			Err:TC=1
A.2048.S	dig @<IP> +retry=0 +qr +bufsize=2048 +edns=0 +ignore s.txt TXT			Rsp:400 bytes
A.2048.M	dig @<IP> +retry=0 +qr +bufsize=2048 +edns=0 +ignore m.txt TXT			Rsp:800 bytes
A.2048.L	dig @<IP> +retry=0 +qr +bufsize=2048 +edns=0 +ignore l.txt TXT			Rsp:1600 bytes
A.2048.XL	dig @<IP> +retry=0 +qr +bufsize=2048 +edns=0 +ignore xl.txt TXT			Err:TC=1
A.2048.XXL	dig @<IP> +retry=0 +qr +bufsize=2048 +edns=0 +ignore xxl.txt TXT			Err:TC=1
A.4096.S	dig @<IP> +retry=0 +qr +bufsize=4096 +edns=0 +ignore s.txt TXT			Rsp:400 bytes
A.4096.M	dig @<IP> +retry=0 +qr +bufsize=4096 +edns=0 +ignore m.txt TXT			Rsp:800 bytes
A.4096.L	Dig @<IP> +retry=0 +qr +bufsize=4096 +edns=0 +ignore l.txt TXT			Rsp:1600 bytes
A.4096.XL	Dig @<IP> +retry=0 +qr +bufsize=4096 +edns=0 +ignore xl.txt TXT			Rsp:2400 bytes
A.4096.XXL	Dig @<IP> +retry=0 +qr +bufsize=4096 +edns=0 +ignore xxl.txt TXT			Rsp:3200 bytes
	DNSSEC-Signed Domain Compatibility			
B.NF.X	Dig @<IP> +retry=0 +qr	signed.	SOA	Rsp:AD=0,CD=0
B.NF.U	Dig @<IP> +retry=0 +qr	UnSiGNED.	SOA	Rsp:AD=0,CD=0 *
	DNSSEC Request Flag Compatibility			
E.A1C0.X	Dig @<IP> +retry=0 +qr +adflag	signed.	SOA	Rsp:AD=1,CD=0 **
E.A0C1.X	Dig @<IP> +retry=0 +qr +cdflag	signed.	SOA	Rsp:AD=0,CD=1
E.A1C1.X	Dig @<IP> +retry=0 +qr +adflag +cdflag	signed.	SOA	Rsp:AD=0,CD=1
E.A1C0.U	Dig @<IP> +retry=0 +qr +adflag	unsigned.	SOA	Rsp:AD=0,CD=0
E.A0C1.U	Dig @<IP> +retry=0 +qr +cdflag	unsigned.	SOA	Rsp:AD=0,CD=1
E.A1C1.U	Dig @<IP> +retry=0 +qr +adflag +cdflag	unsigned.	SOA	Rsp:AD=0,CD=1
	Checking Disabled (CD) Compatibility			
D.CD.X	Dig @<IP> +retry=0 +qr +dnssec +cdflag	signed.	SOA	Rsp:AD=0,CD=1
D.CD.U	Dig @<IP> +retry=0 +qr +dnssec +cdflag	unsigned.	SOA	Rsp:AD=0,CD=1
	DNSSEC OK (DO) Compatibility			
C.DO.X	Dig @<IP> +retry=0 +qr +dnssec	signed.	SOA	Rsp:AD=1,CD=0
C.DO.U	Dig @<IP> +retry=0 +qr +dnssec	unsigned.	SOA	Rsp:AD=0,CD=0
	No Open Resolver			
F.OPEN	Dig @<IP> +retry=0 +qr	.	SOA	Timeout or Deny

* In B.NF.U, mixed-case name used to check whether resolver copies 0x20 bit

** In E.A1C0.X, BIND 9.5.0-P1 returns AD=1, while BIND 9.4.2 returns AD=0

*** In A.x.x, +ignore used to avoid fail-over to TCP after expected truncations

In Test Series T, responses are simply used to document the unit's support for TCP and UDP. Resolver version is also retrieved from units that permit that query.

In Test Series A, units are expected to return the specified small (S), medium (M), large (L), extra large (XL), and XXL response lengths for UDP/EDNS0 queries. Where lengths exceed the specified buffer size, successful responses must indicate that expected error by setting the truncation flag. Failure conditions include silently dropping the request, rejecting the request with FORMERR, returning TC=1 when response length is less than bufsize, returning malformed truncated responses without setting TC, or persistent timeouts.

In Test Series B, C, D, and E, units are expected to return valid responses of correct length and content for both signed and unsigned test domains. Flags are checked as specified in the Success column above; units are generally expected to pass the response flags returned by the resolver without modifying them. Failure conditions include silently dropping the request, rejecting OPT RR requests with FORMERR, failing to pass the client's request flags to the resolver, and failing to return the resolver's entire answer (including DNSSEC flags, RRSIGs, and Authorities) to the client.

Test F.OPEN is the only test that is considered a Success if the query times out or is explicitly denied (e.g., "WARNING: recursion requested but not available"). Returning an actual TXT response record for the requested domain is considered Failure.

To assess source port randomization, we ran tests available at http://www.doxpara.com and https://www.dns-oarc.net/oarc/services/porttest and recorded the OARC score (standard deviation < 296 is rated "Poor," while > 3980 is rated "Great").

Note: Dig command defaults that can be assumed when not specified above:

-4	IPv4 transport only
+recurse	Recursion desired
+time=5	Don't wait longer than 5 seconds for response
+nodnssec	DO flag disabled (non-DNSSEC query)
+nocdflag	CD flag disabled (server-side checking disabled)
+noadflag	AD flag disabled (non-authenticated data returned)