Improving Response Deliverability in DNS(SEC)

Gijs van den Broek[*‡], Roland van Rijswijk[‡], Aiko Pras[*], Anna Sperotto[*]

[*]University of Twente, Enschede, The Netherlands
[‡]SURFnet bv, Utrecht, The Netherlands

Gijs van den Broek
Graduate Intern at SURFnet

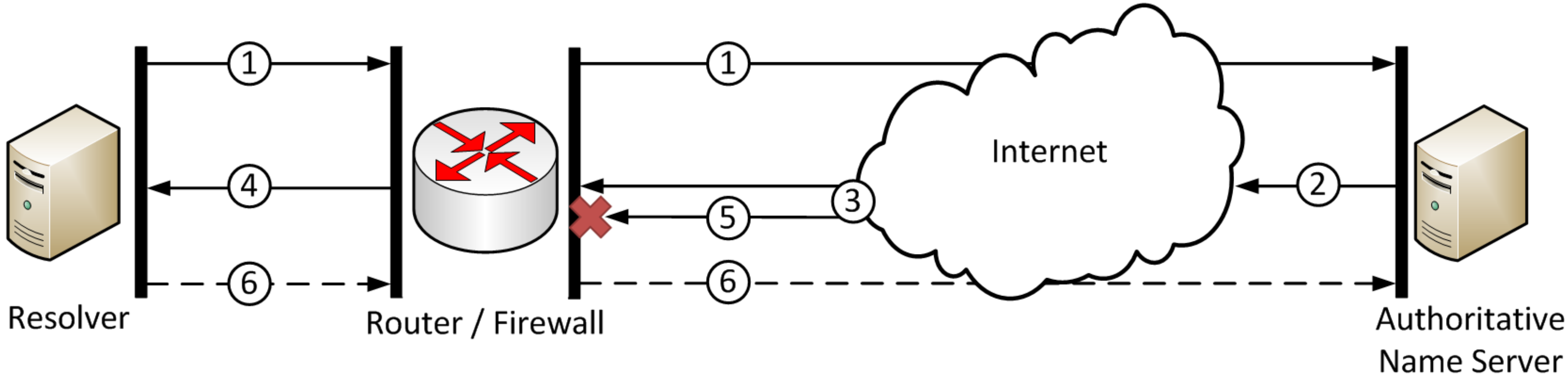
SURF NET

UNIVERSITY OF TWENTE.

Contents

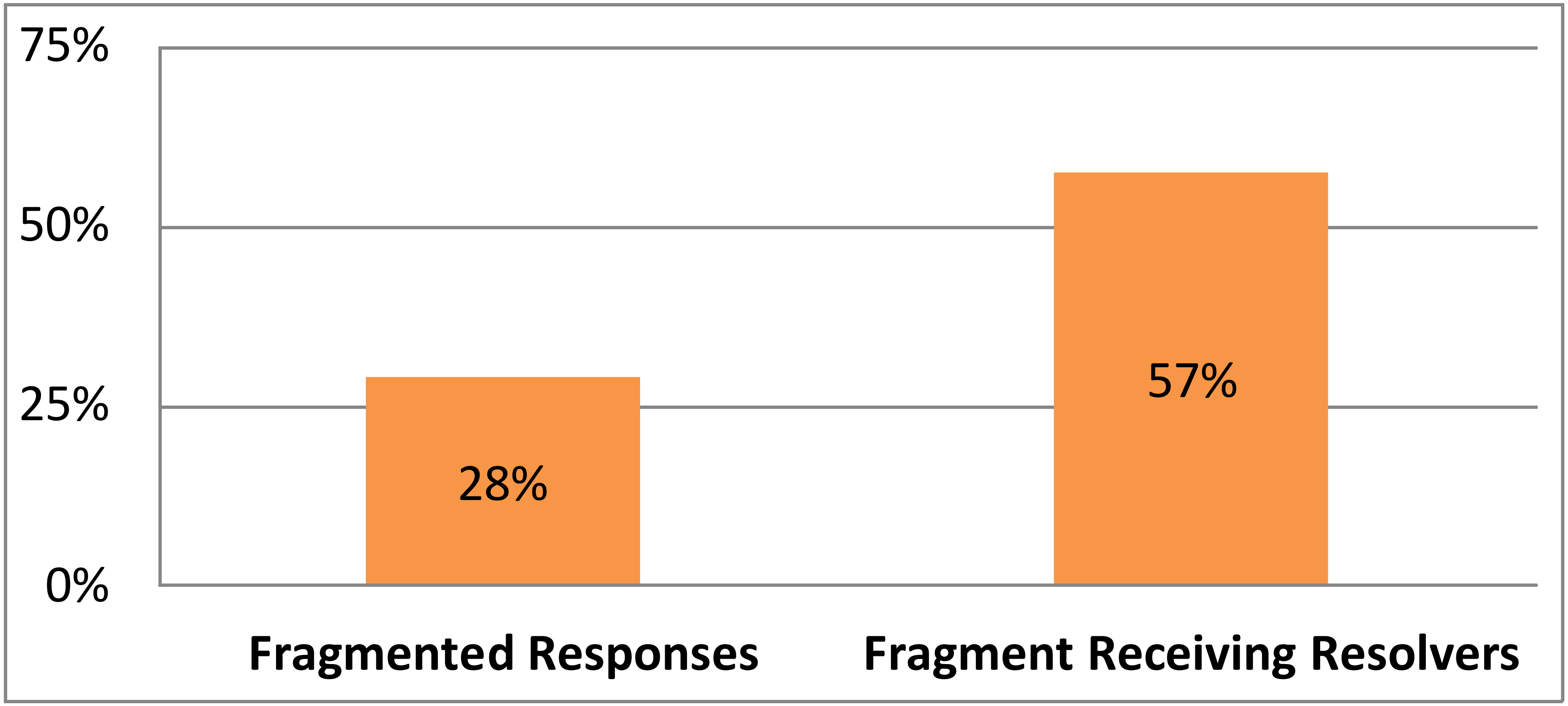
- Problem Overview
- Extent of the Problem
- Proposal for Two Solutions
- Comparison
- Q&A

Problem Overview



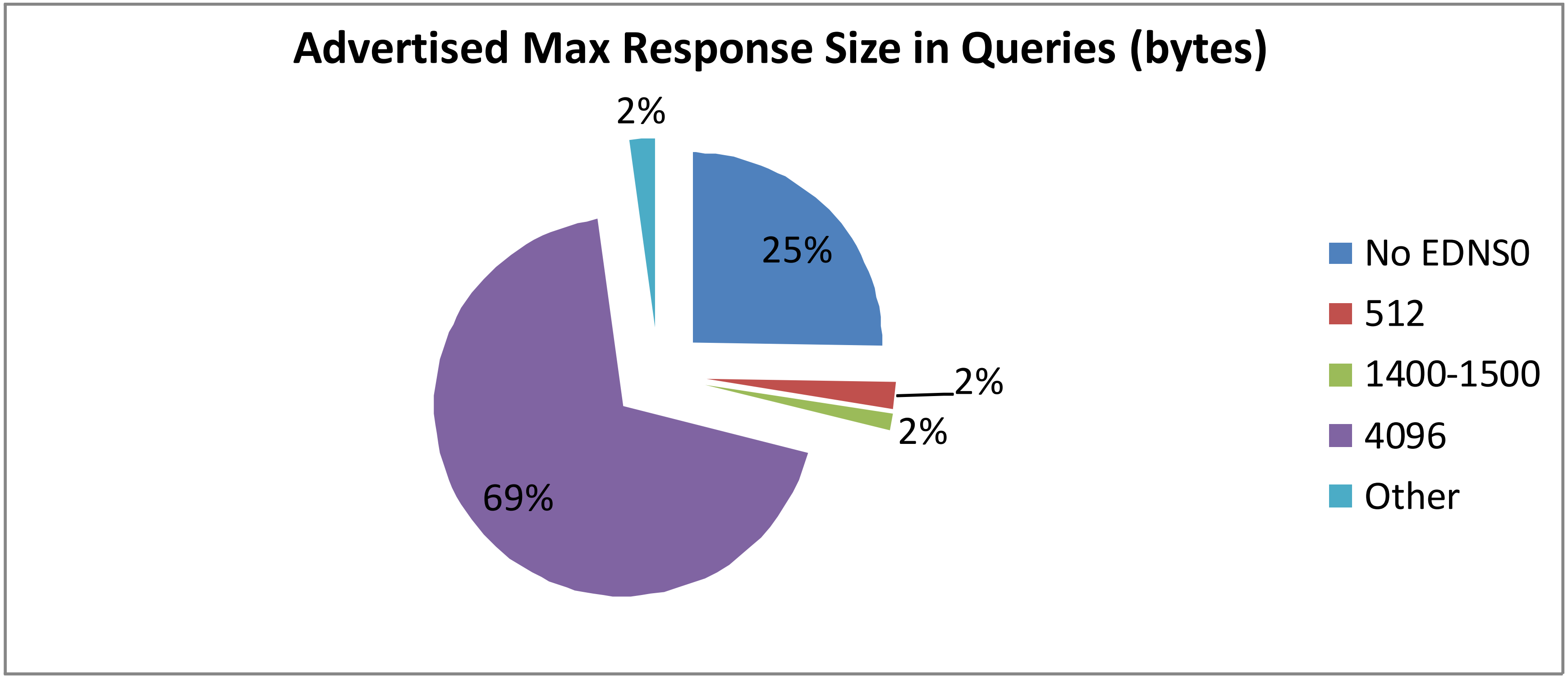
	Description
1	DNS query sent to authoritative name server
2	DNS response returned
3	DNS response fragmented into IP fragments due to lower MTU
4	First IP fragment of DNS response arrives at resolver
5	Second IP fragment of DNS response is blocked at firewall
6	An ICMP Fragment Reassembly Time Exceeded message is sent 30 seconds later

Extent of the Problem (1/3)



Percentage of all UDP DNS responses being fragmented and percentage of all resolvers receiving fragments (measured at ns3.surfnet.nl)

Extent of the Problem (2/3)



EDNS0 Headers in DNS queries contain a field ‘Maximum UDP Payload’ [1], indicating the maximum response size for the querying resolver (measured at ns3.surfnet.nl)

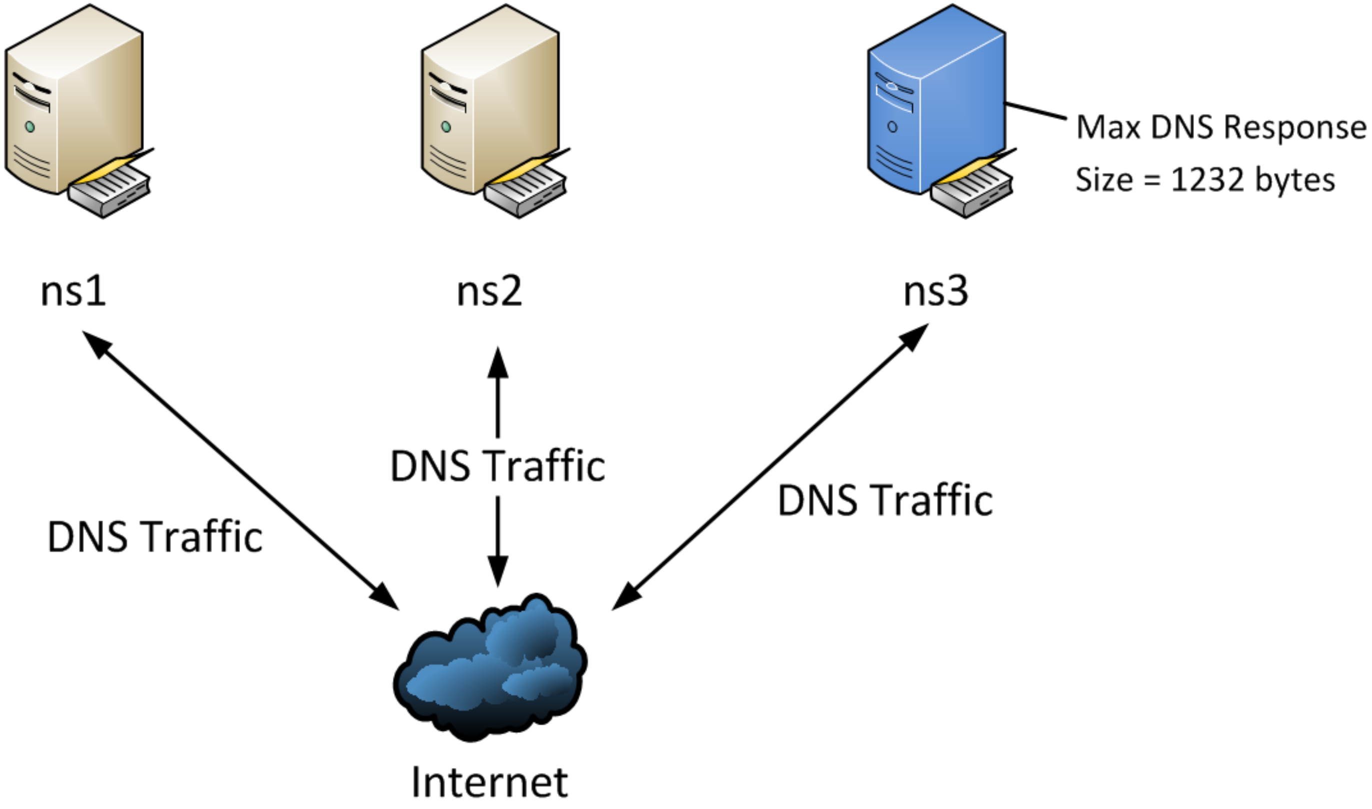
Extent of the Problem (3/3)

Resolver Behavioural Characteristics	Unique Resolvers
Case 1: Sending ICMP Fragment Reassembly Time Exceeded (FRTE)	1.1%
Case 2: Removal of EDNS0 header in retries	2.4%
Case 3: Retries for large (>512 bytes) responses exceed 4%	9.7%
Case 4: Reduced advertised buffer size in retries	3.5%
Case 5: TCP fallback w/o truncated UDP response preceding it	<0.1%

Note 1: these cases are not mutually exclusive

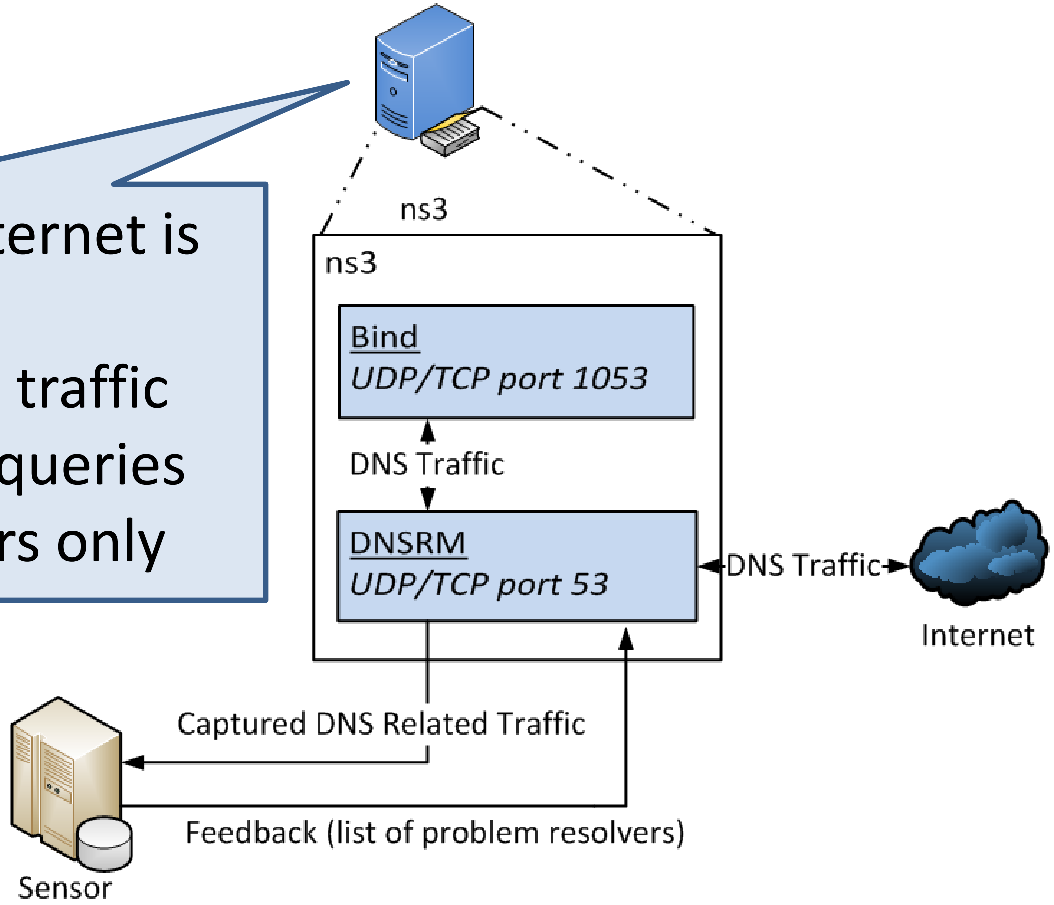
Note 2: an estimated 9% of all hosts cannot receive fragmented UDP [2]. We will likely see a lower value, since we consider the perspective of an authoritative name server, which predominantly handles queries from (caching) resolvers from ISPs

Solution 1


Max DNS Response
Size = 1232 bytes
ns1
ns2
ns3
DNS Traffic
DNS Traffic
DNS Traffic
Internet

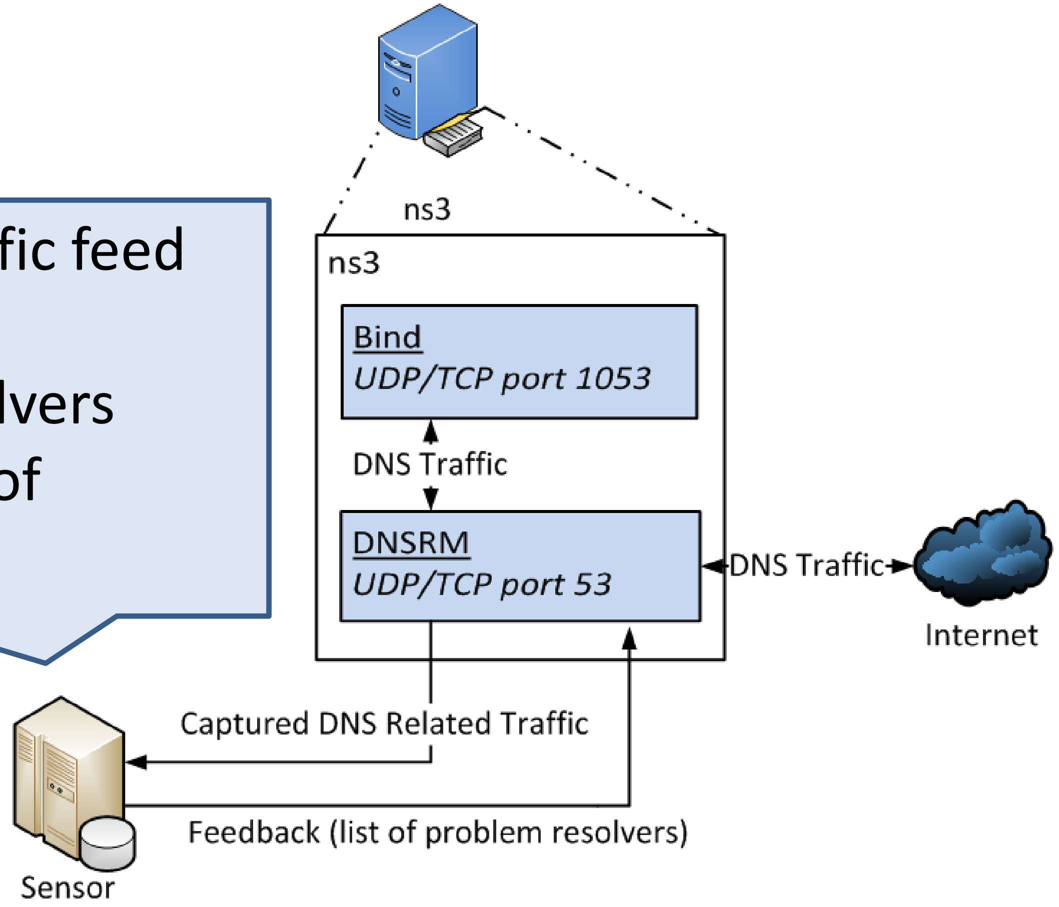
Solution 2 – Name Server

- Between BIND and Internet is DNSRM as host proxy
- DNSRM forwards DNS traffic feed to sensor; alters queries from problem resolvers only

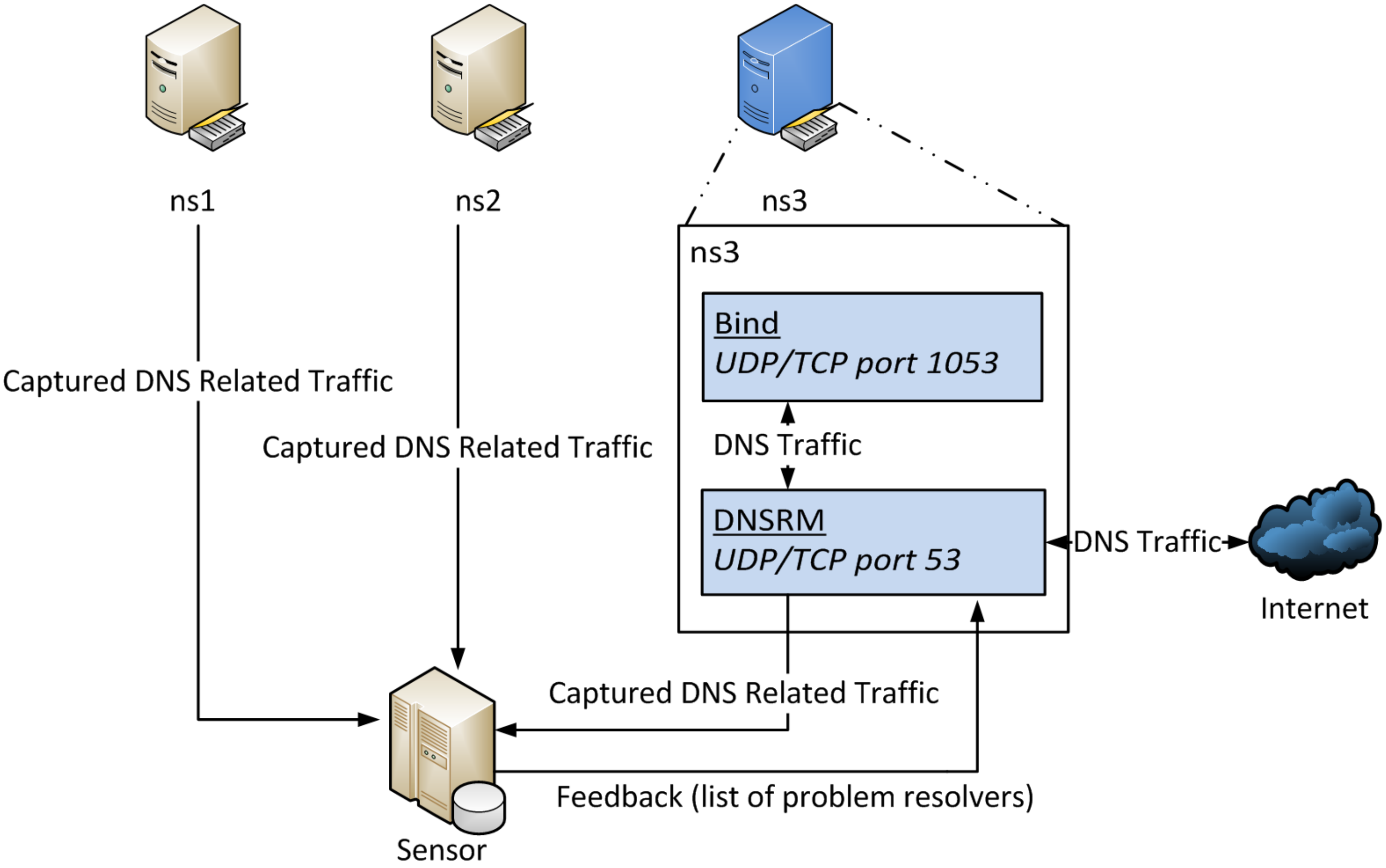


Solution 2 - Sensor

- Receives live DNS traffic feed from name servers
- Detects problem resolvers
- Returns IP addresses of problem resolvers



Solution 2 - Overview


ns1
ns2
ns3
ns3
Bind
UDP/TCP port 1053
DNS Traffic
DNSRM
UDP/TCP port 53
DNS Traffic
Internet
Captured DNS Related Traffic
Captured DNS Related Traffic
Captured DNS Related Traffic
Feedback (list of problem resolvers)
Sensor

Comparison of Experiments

- **Solution 1**
  - Very simple (i.e. usually limited to one server variable)
  - Affects every querying resolver
  - Rewards bad behaviour, ‘punishes’ good behaviour

- **Solution 2**
  - More complex setup required
  - Affects only problem resolvers
  - To some extent problem resolvers keep feeling the pain by not helping them intermittently

Final Remarks

- Problems with fragmented DNS responses are not limited to DNSSEC
- At least 1%* of all resolvers will be marked as a problem resolver, likely much more
- Issues with EDNS0 headers and UDP packets > 512 bytes in some firewalls/routers may remain [3]

* Preliminary results

✉ j.g.vandenbroek@student.utwente.nl

in jgvandenbroek

W dnssec.surfnet.nl

SURF NET

UNIVERSITY OF TWENTE.

References

[1] Vixie, RFC 2671: “Extension Mechanisms for DNS (EDNS0)”, chapter 4.5, August 1999

[2] Weaver, et al.: “Implications of Netalyzr’s DNS Measurements”, April 2011

[3] Bellis, et al.: “Test Report: DNSSEC Impact on Broadband Routers and Firewalls”, Nominet, September 2008