Measuring DNSSEC Configuration of Upstream Resolvers with RIPE Atlas

Moritz Müller | RIPE 72 Copenhagen – MAT WG

2016-05-25

SIDN LABS

SIDN

- Domain name registry for .nl ccTLD
- SIDN Labs is the R&D team of SIDN
- > 5.6 million domain names
- 2.5 million domain names secured with DNSSEC

Background

Problem:

- 2.5 Million signed .nl domain names but only a few validating resolvers

Goal:

- Improving DNSSEC deployment at upstream resolvers of (Dutch) ISPs

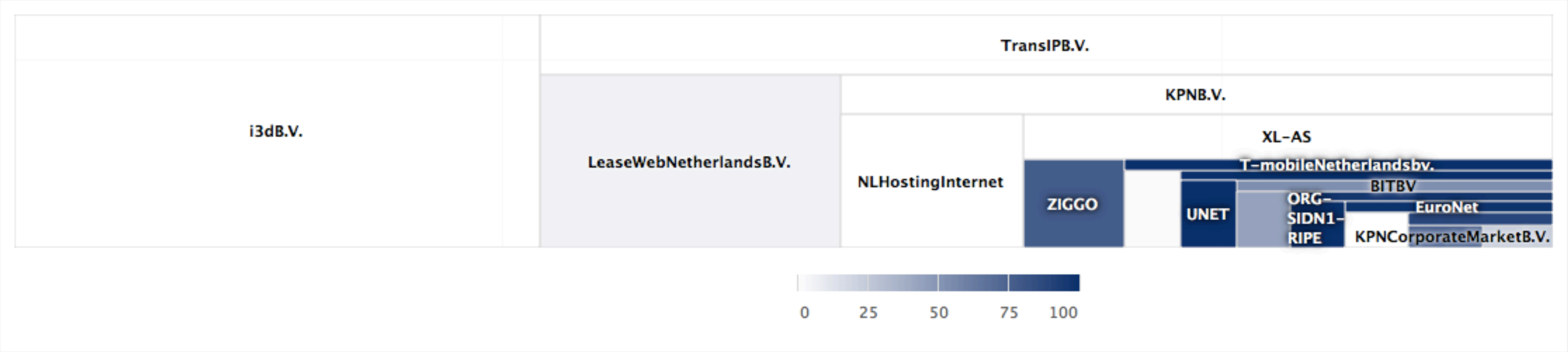
First approach: Passive Measurements

Observe DNS query type at authoritative .nl resolvers

- If:
  - Resolvers ask at least 1.000 times per month for DS or DNSKEY record and has DO bit set
- Then:
  - We label resolver as a validating resolver

First approach: Passive Measurements

- Downsides:
  - Not precise (not sure which resolvers are actually the upstream resolvers of the ISPs)
  - Not sure what resolvers are doing with DNSSEC records (Do they validate? Are they in permissive mode?)



Screenshot from stats.sidnlabs.nl

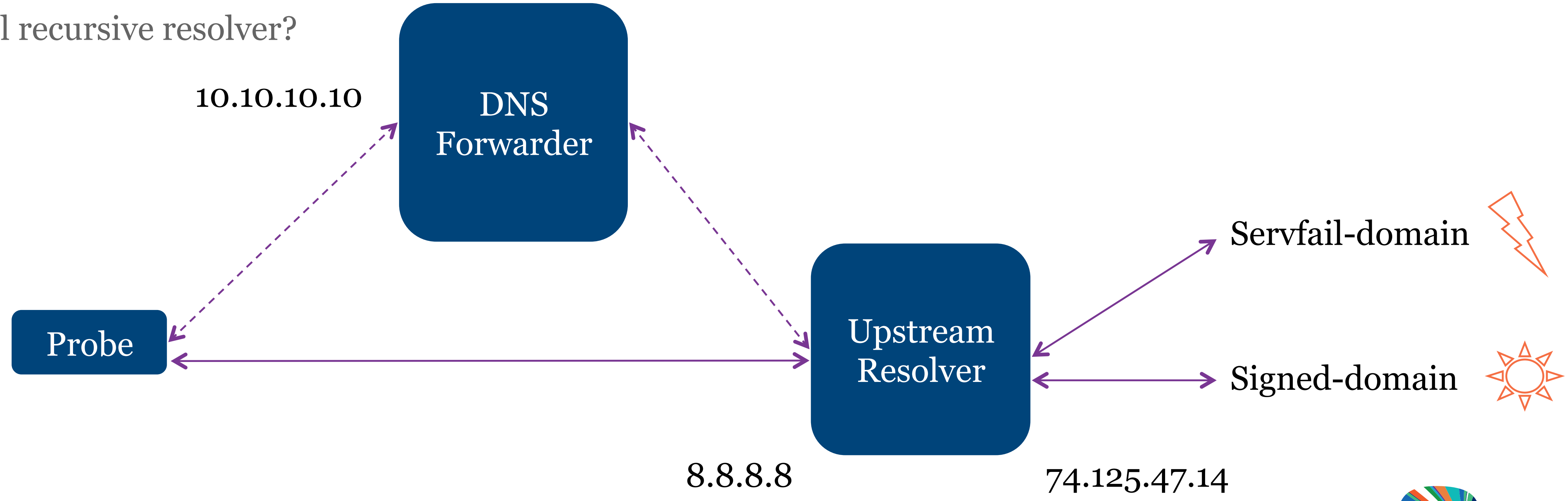
Second approach: Active Measurements - Setup

- Select 500 RIPE Atlas Probes in NL to resolve signed domain and “servfail” domain
- Do bit set
- Use the probe's list of local resolvers

Resolver is:	*Validly Signed Domain*	*AD bit*	*Servfail Domain*
Non-validating	Rcode 0	No	Rcode 0
Validating	Rcode 0	Yes	Servfail
Permissive Mode	Rcode 0	Yes	Rcode 0

Challenges (1/2)

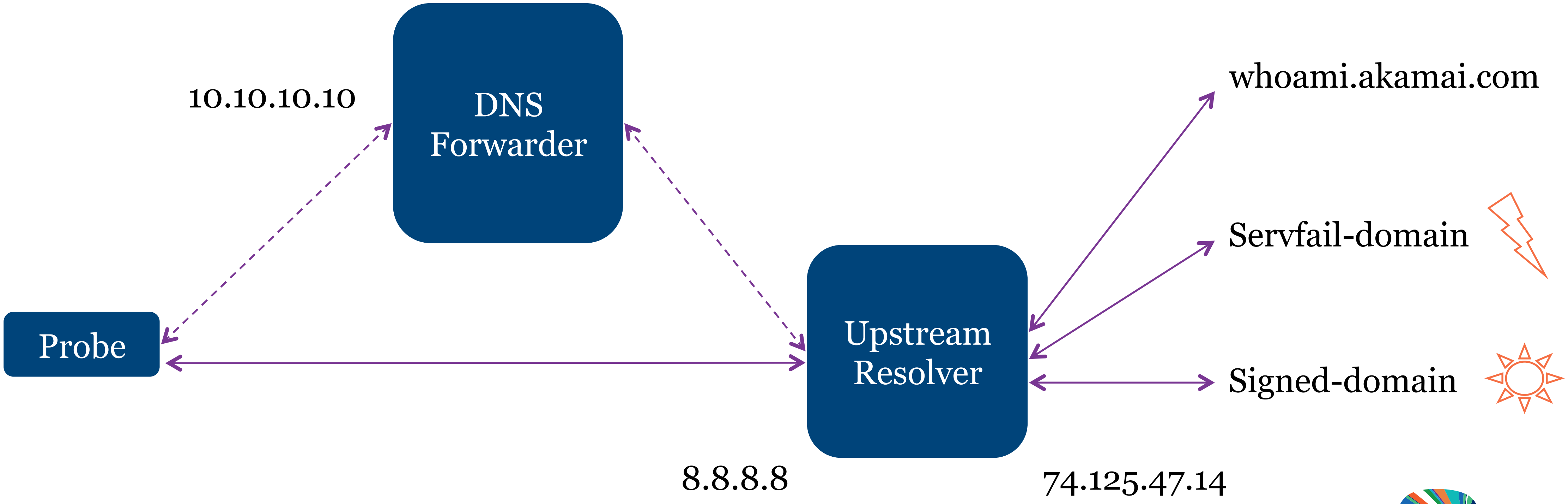
- Which resolver is handling the queries?
  - An upstream resolver of an ISP?
  - A DNS forwarder/proxy?
  - Local recursive resolver?



Challenges (1/2)

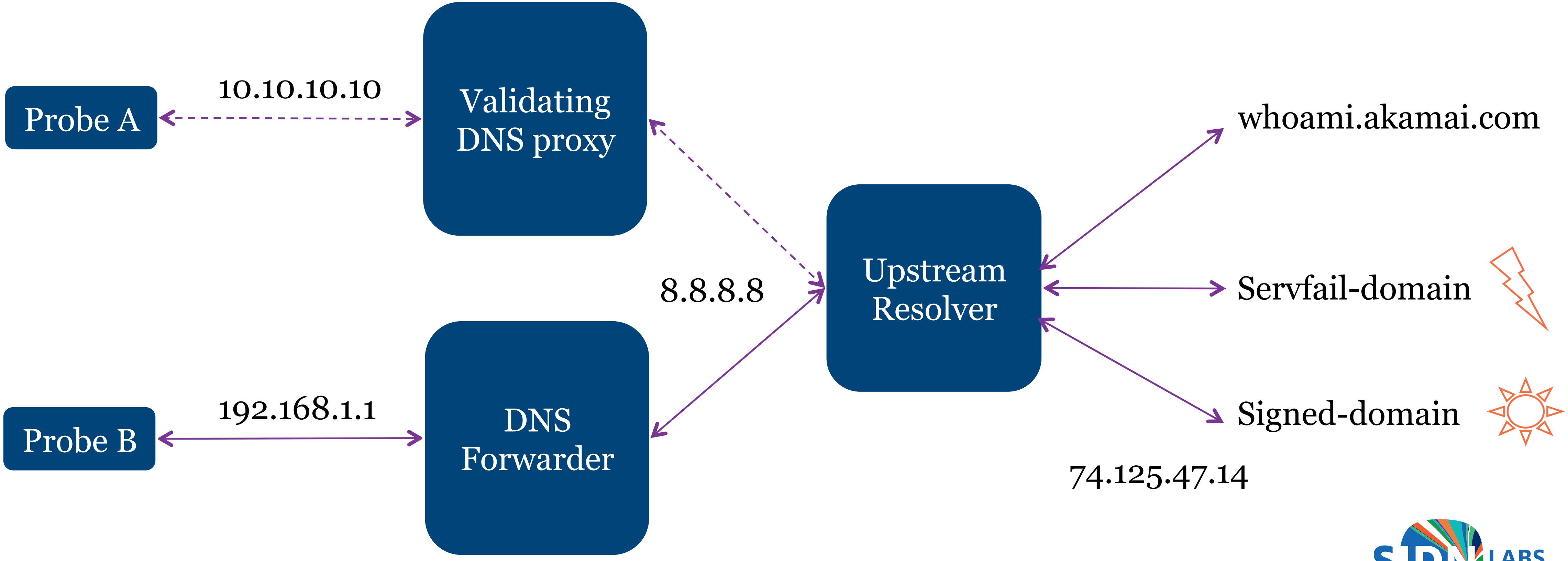
- Which resolver is handling the queries?

→ Third measurement to whoami.akamai.com



Challenges (2/2)

- Validating DNS proxies (like Dnsmasq)
- Contradicting measurement results



Results after 5 weeks of RIPE Atlas Measurements

- 65 unique resolvers (IPs) with at least 1.000 queries and used by 2 probes or more (154 total)
- 9 unique Autonomous Systems
- 24 validating and 41 non-validating resolvers
- 6 % of queries from validating resolvers

Conclusions

- 12 % DNSSEC validation measured by APNIC [1] vs. 6 % by our measurement
- Only a small set of resolvers measured
  - No resolvers of mobile networks
  - Some Dutch ISPs missing
- Measurements: 3671531, 3671532, 3671533

Future Work

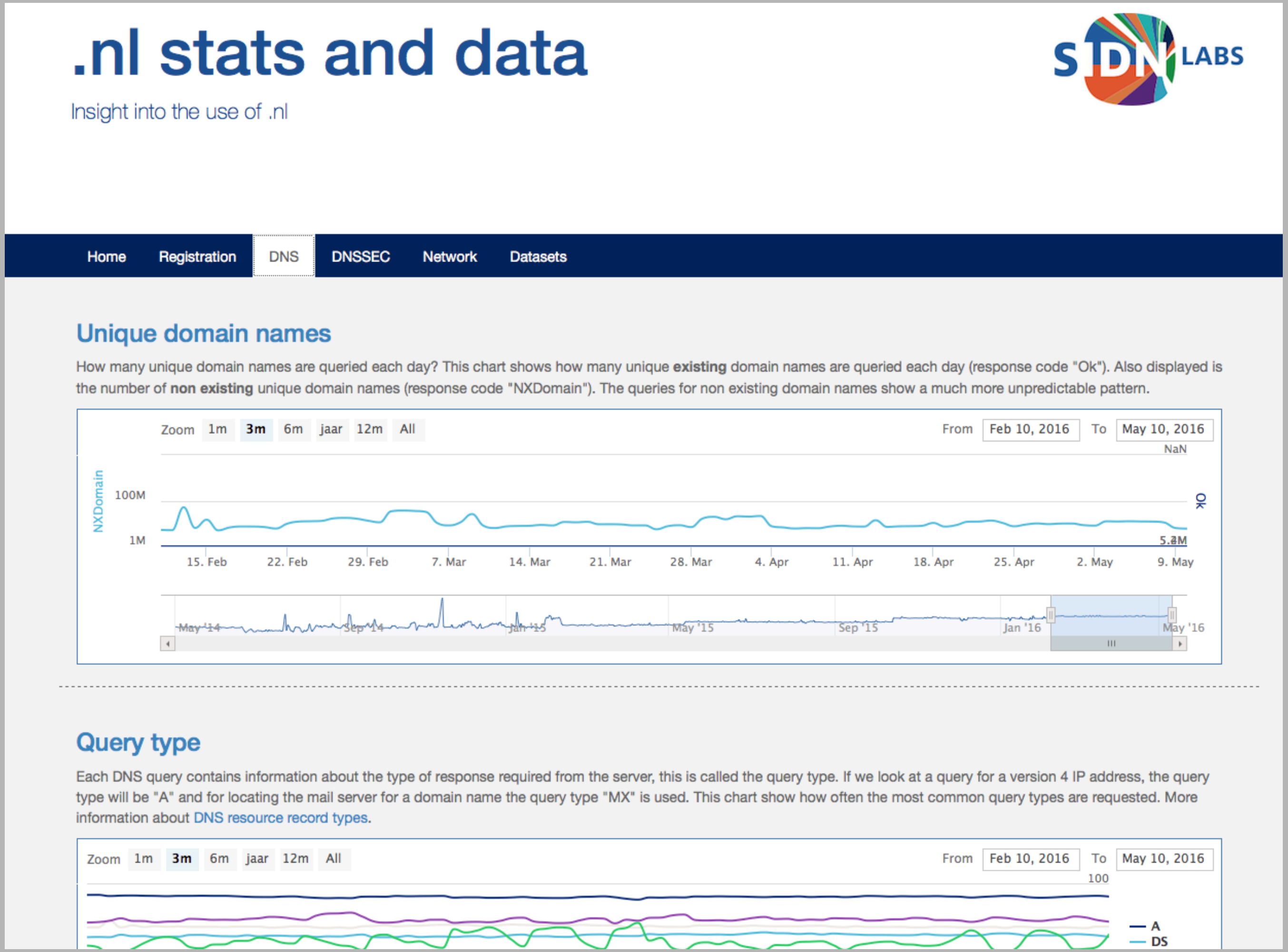
- Analyse the different between our measurements and APNIC's
- Encourage ISPs to roll out DNSSEC at their resolvers
- Measure deployment over time
- Feedback from ISPs

[1] http://stats.labs.apnic.net/dnssec/NL

Moritz Müller

Research Engineer

moritz.muller@sidn.nl



.nl stats and data

Insight into the use of .nl

Unique domain names

How many unique domain names are queried each day? This chart shows how many unique **existing** domain names are queried each day (response code "Ok"). Also displayed is the number of **non existing** unique domain names (response code "NXDomain"). The queries for non existing domain names show a much more unpredictable pattern.

Query type

Each DNS query contains information about the type of response required from the server, this is called the query type. If we look at a query for a version 4 IP address, the query type will be "A" and for locating the mail server for a domain name the query type "MX" is used. This chart show how often the most common query types are requested. More information about DNS resource record types.

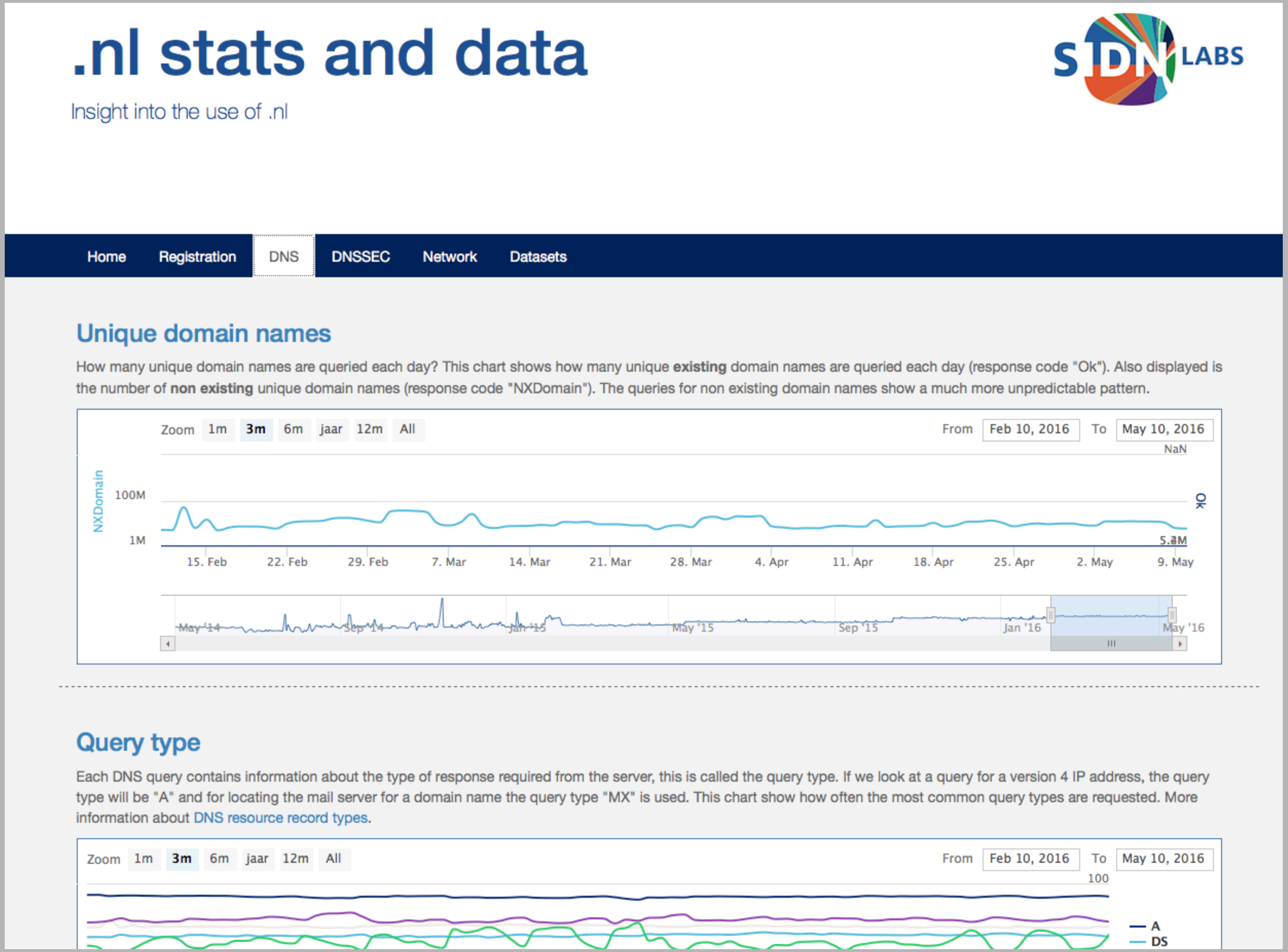
stats.sidnlabs.nl

Moritz Müller

Research Engineer

moritz.muller@sidn.nl

Questions?



.nl stats and data

Insight into the use of .nl

Unique domain names

How many unique domain names are queried each day? This chart shows how many unique **existing** domain names are queried each day (response code "Ok"). Also displayed is the number of **non existing** unique domain names (response code "NXDomain"). The queries for non existing domain names show a much more unpredictable pattern.

Query type

Each DNS query contains information about the type of response required from the server, this is called the query type. If we look at a query for a version 4 IP address, the query type will be "A" and for locating the mail server for a domain name the query type "MX" is used. This chart show how often the most common query types are requested. More information about DNS resource record types.

stats.sidnlabs.nl