SIDN

For confidence online

KSK algorithm rollover for .nl

Stefan Ubbink | OARC42, Charlotte, NC, USA

8 februari 2024

Public

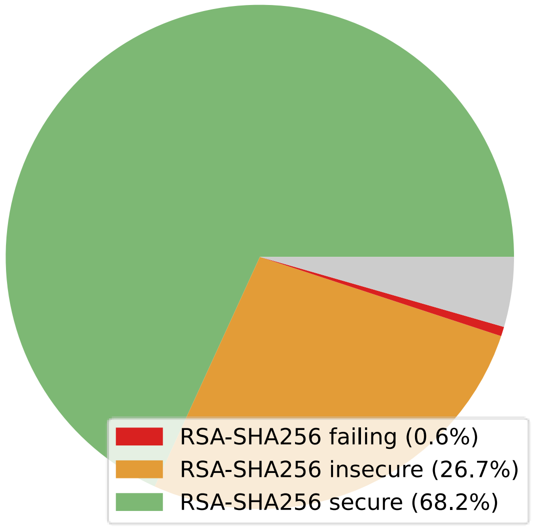
Agenda

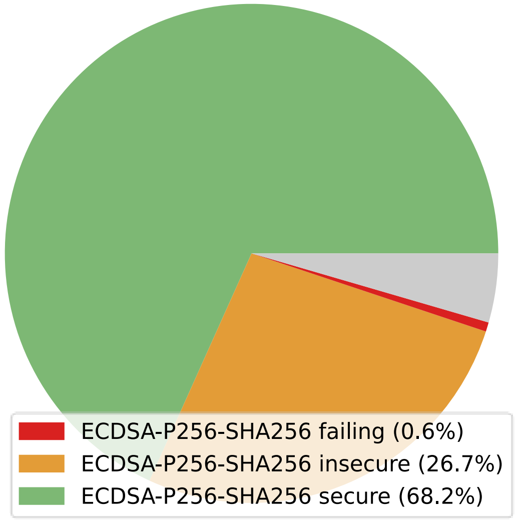
1. Why
2. Preparation
3. Planning
4. Executing
5. Measurements

Photo by Stefan Ubbink

Why?

- Using a safer algorithm
- Keeping up with new recommendations
- Enough support in resolvers
- Smaller DNSSEC answers





Source: https://dnsthought.nlnetlabs.nl

Preparation

- New Thales HSM for better ECDSA performance
- Test, test, test
  - Normal run on test setup, using a fakeroot
  - Local DNSviz
  - Lab setup with fast policy
  - Acceptance with real data and policy
    - Memory usage
    - Time needed for validation of the signed zone

THALES

Building a future we can all trust

Planning

- Based on acceptance run
- Dependencies
  - External parties (IANA)
  - ZSK rollover

Planning

- 4 July: preparation
- 5 July: change OpenDNSSEC policies
- 11 July: Add algo 13 DS to the root zone
- 14 July*: check algo 13 path
- 17 July*: remove algo 8 DS from the root zone
- 19 July*: delete algo 8 keys from OpenDNSSEC.

* dependent on external parties

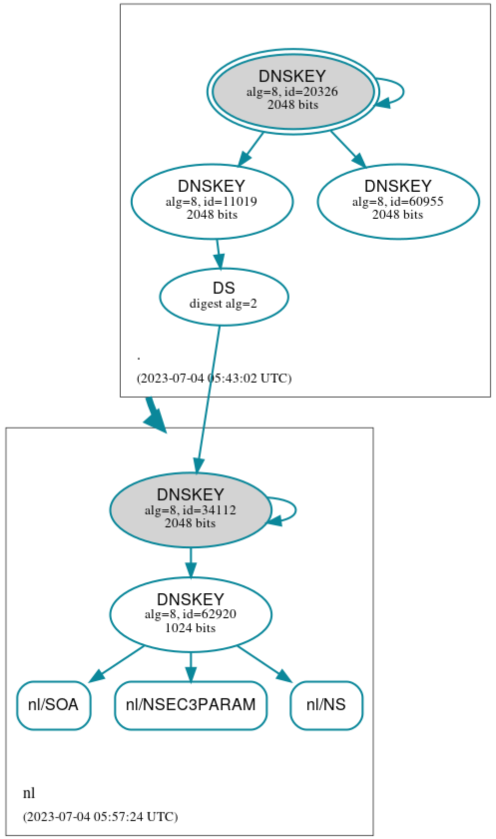
Photo by Alexander Schimmeck on Unsplash

Executing

- Use written plan with commands and checks
- Continual checking
- DNSViz at strategic times
- Go-No go

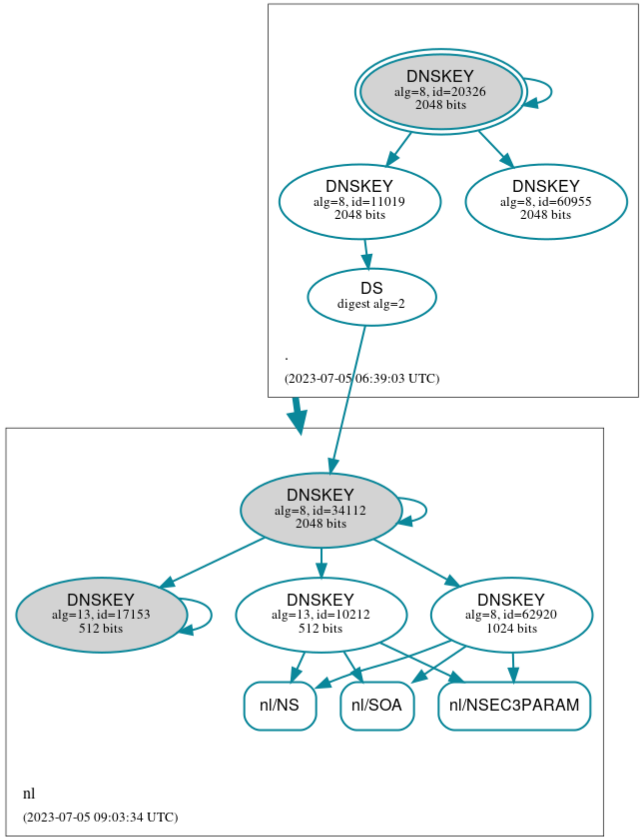
When	.nl size (GB)
Before	4.5
During	6.4
After	3.7

Algorithm 8 situation



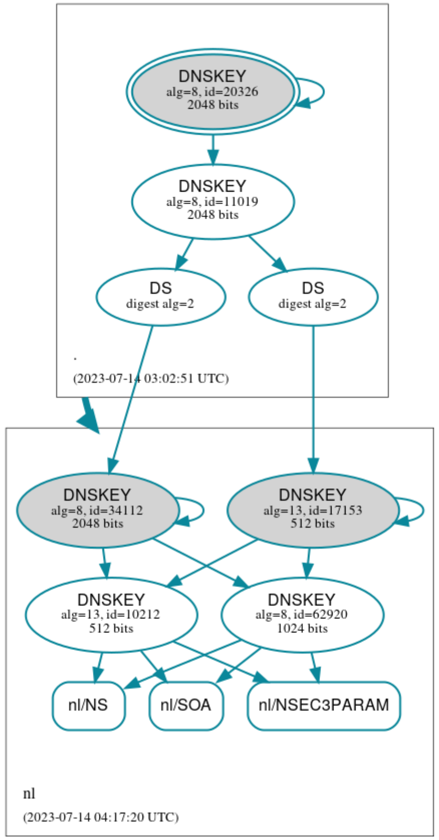
https://dnsviz.net/d/nl/ZKOoxA/dnssec/

Policy change



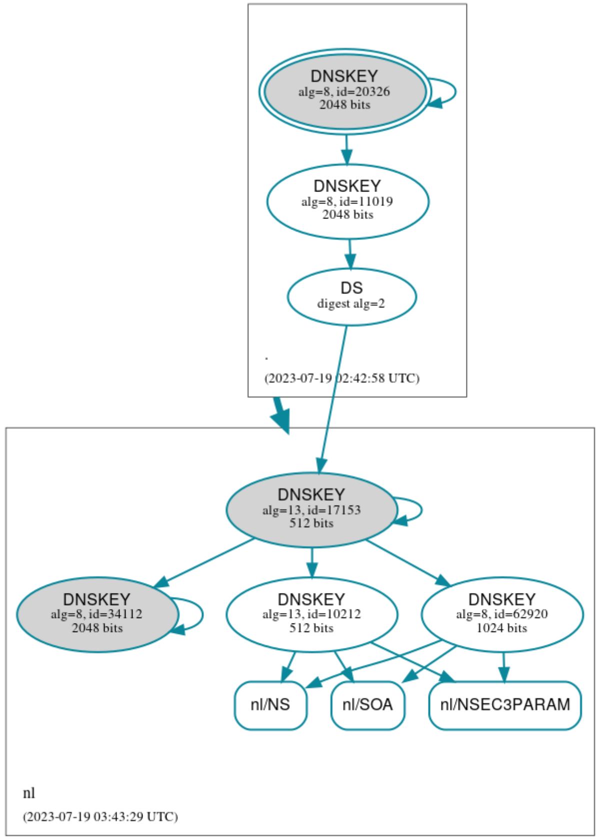
https://dnsviz.net/d/nl/ZKUx5g/dnssec/

Add algorithm 13 DS to root



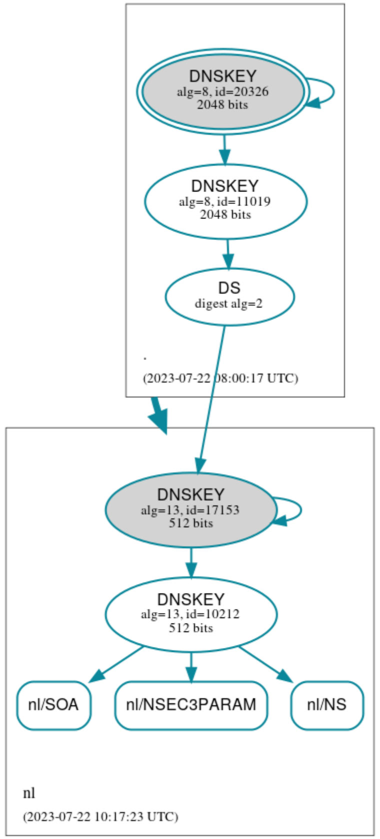
https://dnsviz.net/d/nl/ZLDMUA/dnssec/

Remove algorithm 8 DS from root



https://dnsviz.net/d/nl/ZLdb4Q/dnssec/

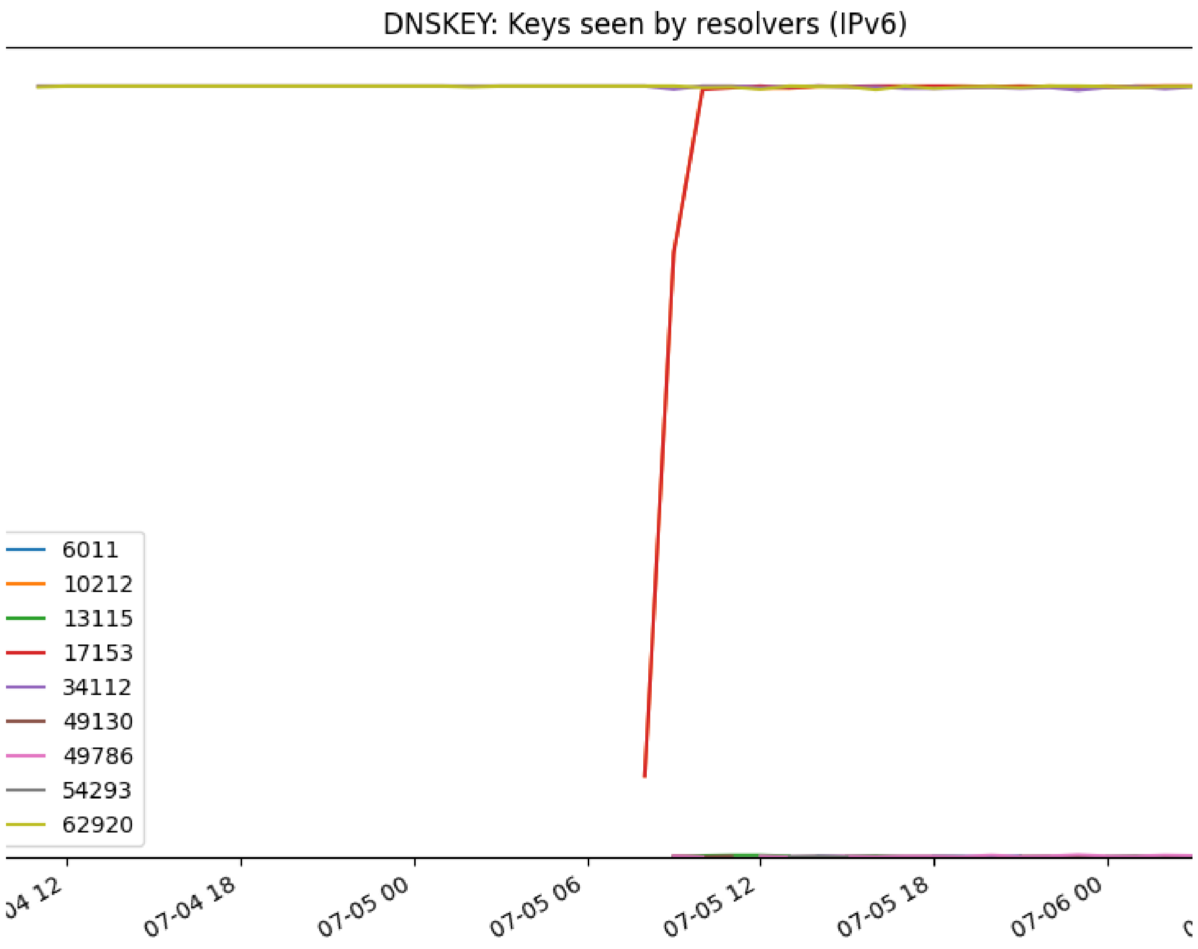
Stop using algorithm 8



https://dnsviz.net/d/nl/ZLuFjA/dnssec/

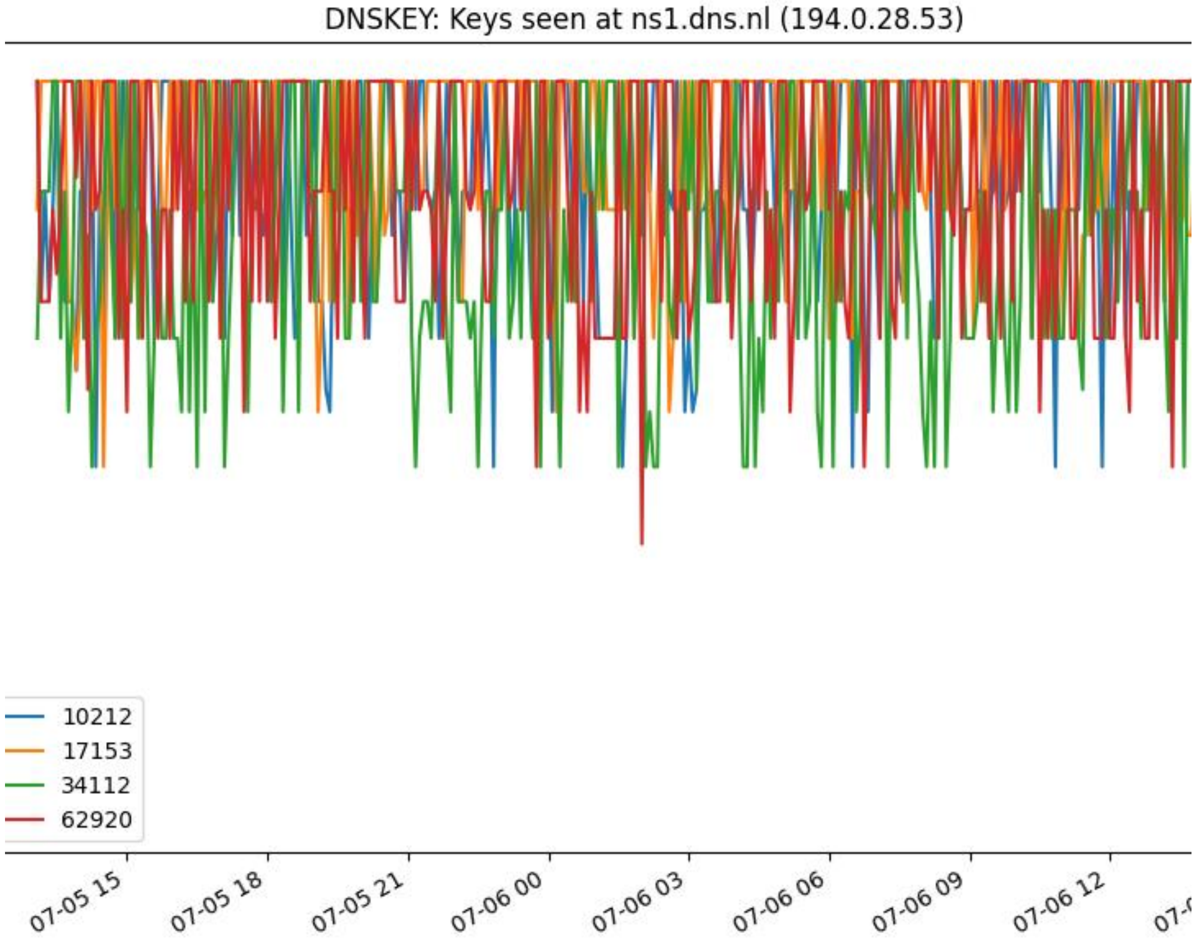
Measurements with RIPE Atlas probes

- Rollovermon
  - Propagation delay for DNSKEY (1/h)
  - Propagation delay for DS (1/d)
  - DNSKEY @nsX.dns.nl (5 min)
  - DS records @root servers (5 min)
  - Trust chain (1/h)
- 17153 = EC KSK



Measurements

- Strange measurements
- Caused by
  - Small buffersize
  - Trying to get key ID from fragments



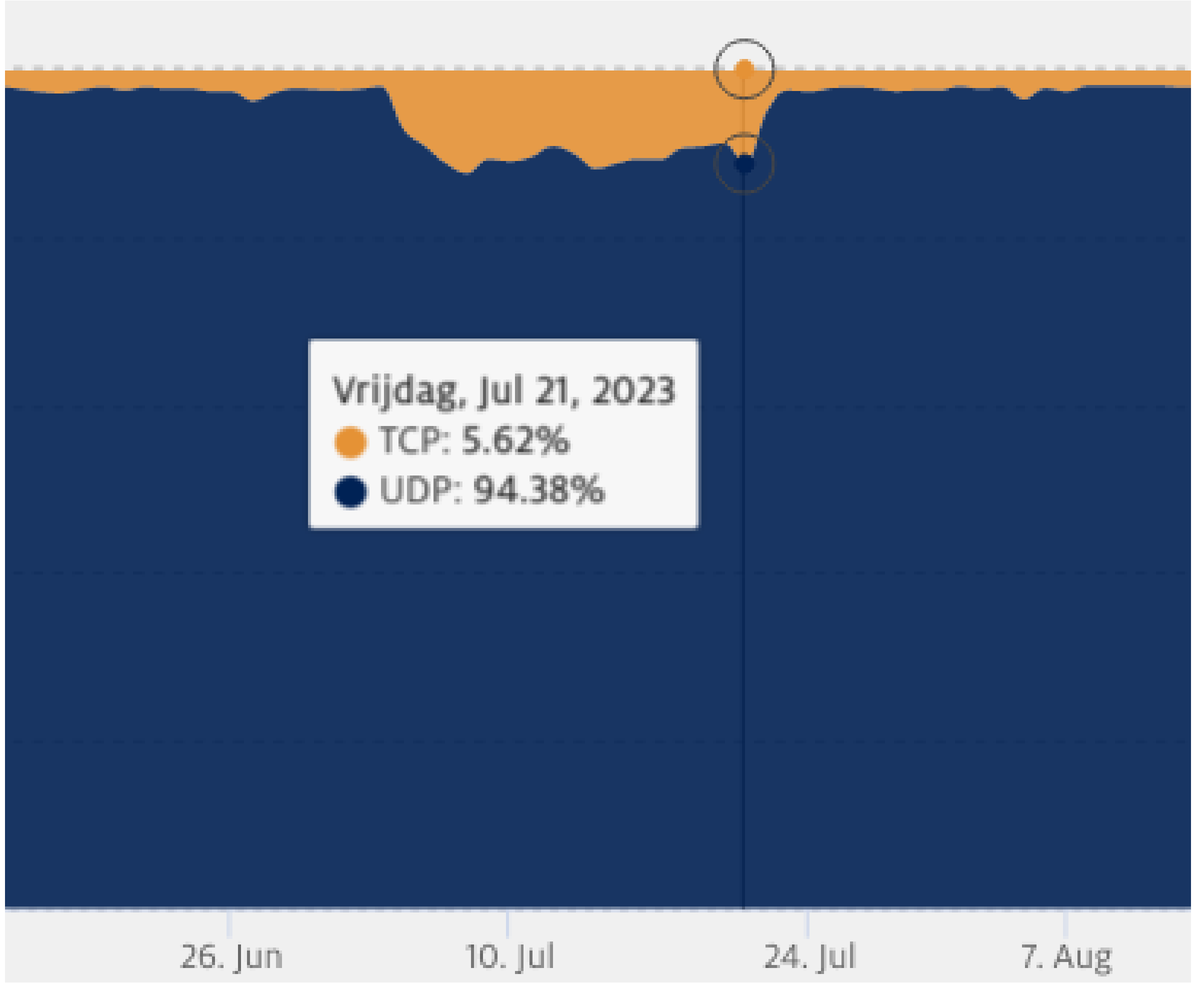
Response sizes in bytes*

Type	Before	During	After
NXDOMAIN	1015	1402	759
DNSKEY	766	1024	310
NS	1214	1022	928

* Only showing sizes from ns1.dns.nl (v6 and v4), based on DNSviz data, other implementations differ

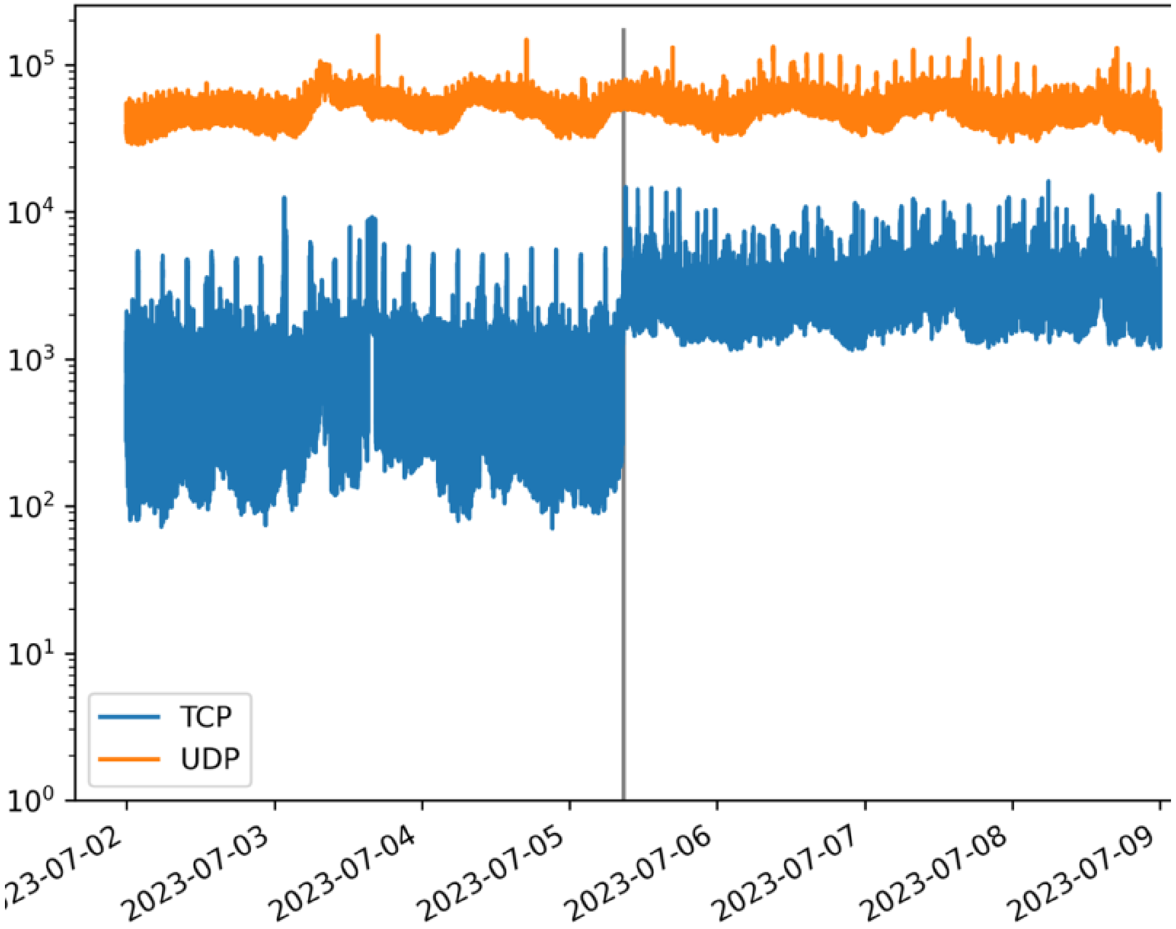
Change in TCP traffic

- Before: ~1% TCP queries (~359 qps)
- During: ~5% TCP queries (~2421 qps)
- After: ~1 % TCP queries



Source: stats.sidnlabs.nl

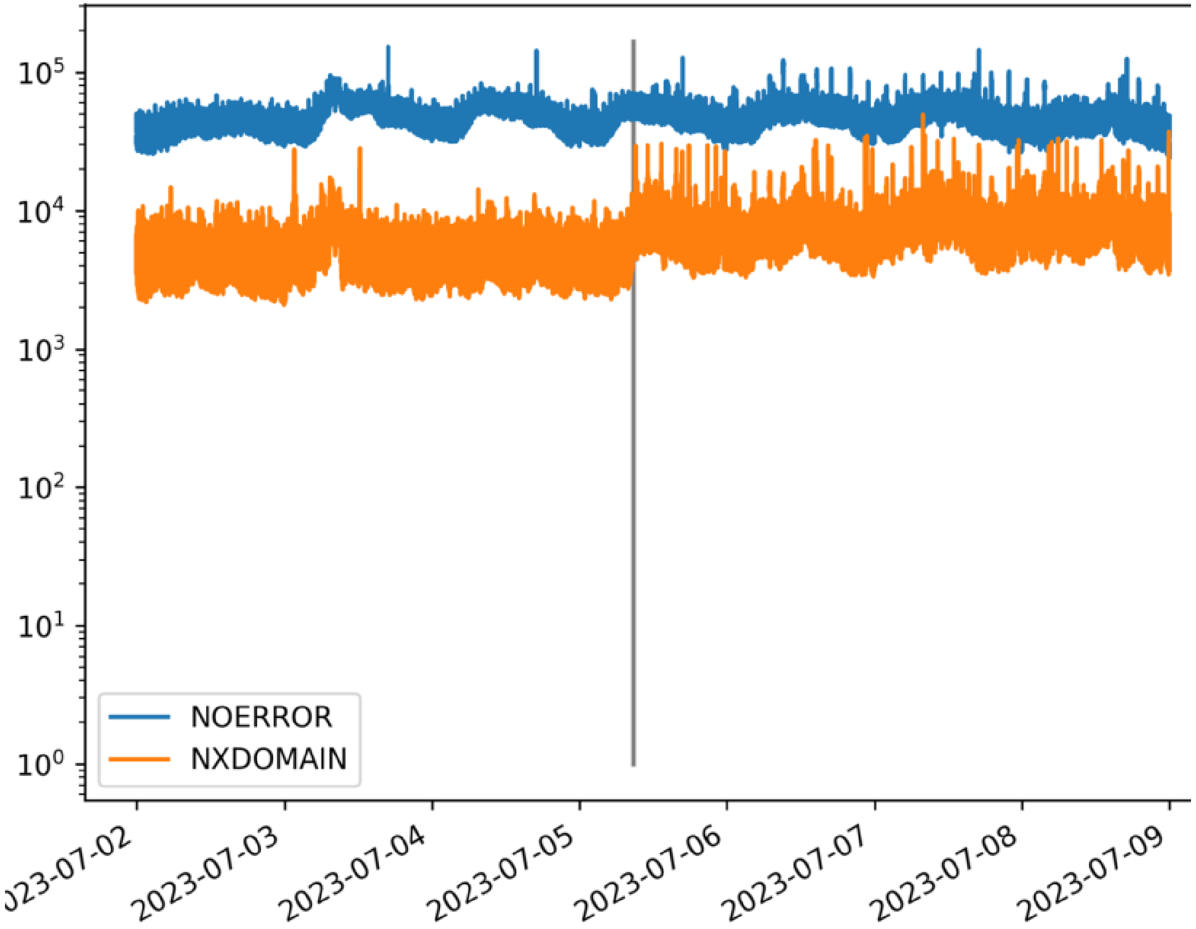
Change in TCP traffic



Lack of TCP support

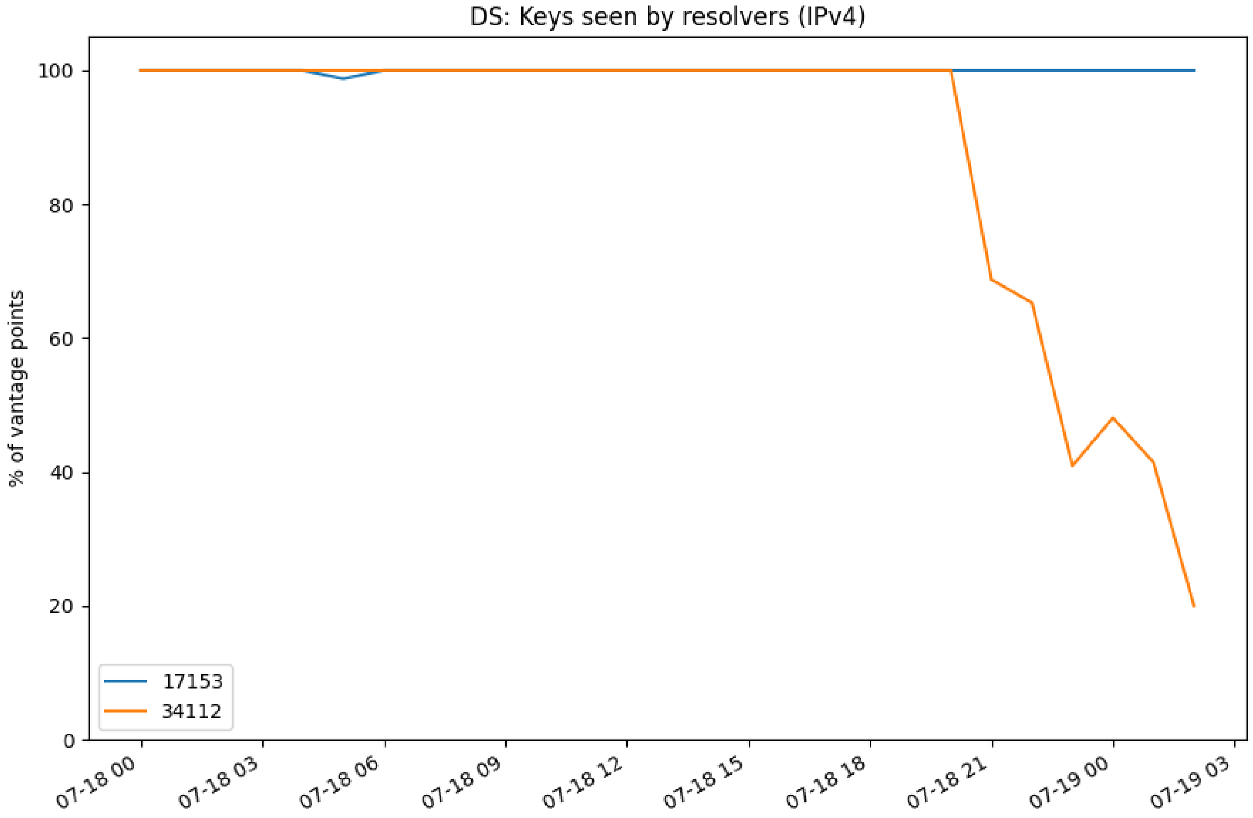
- Increase of 1.6 times
- 25% had an increase of 8 times

- Keep asking via UDP
- University measurements
- Impact unknown
- No failure reports

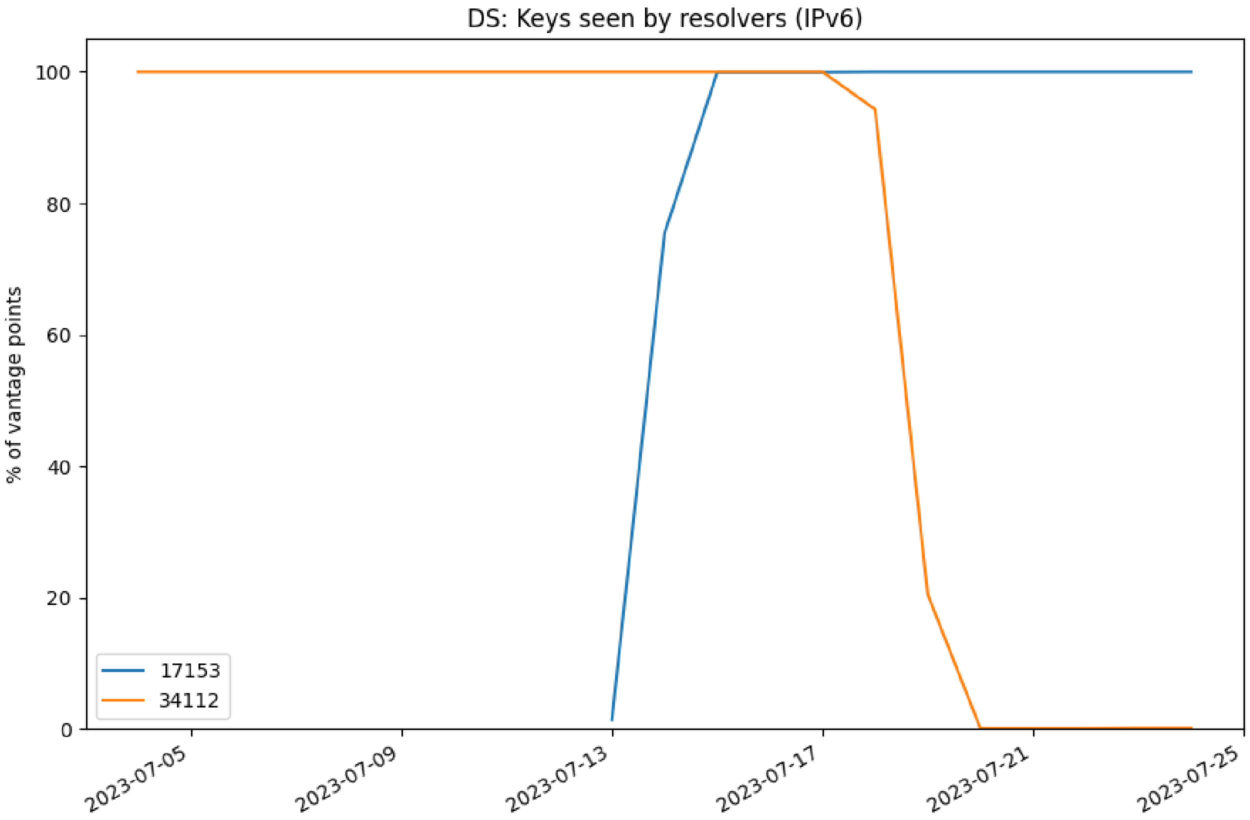


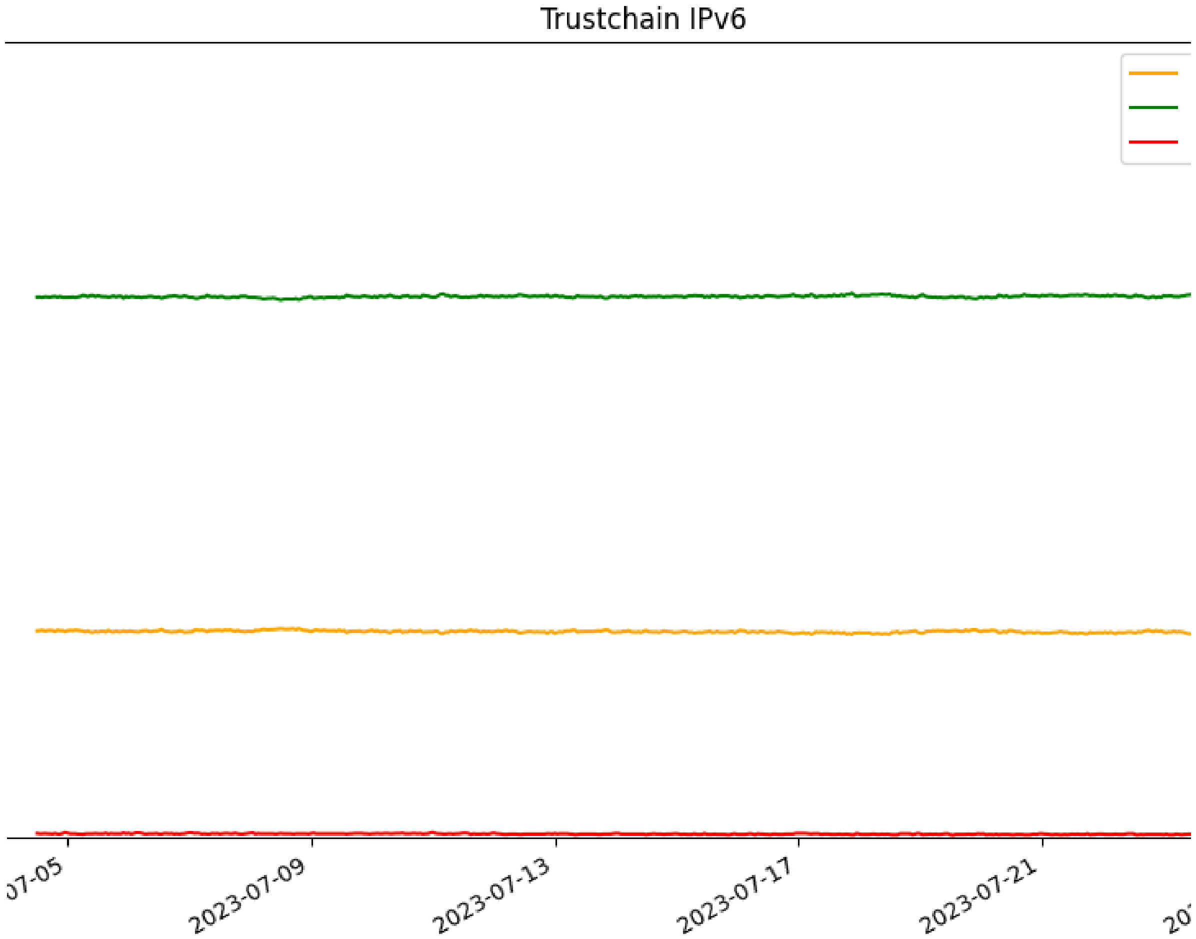
Measurements

- Removing the RSA KSK



No measured impact





Are there any questions?

Follow us

SIDN.nl

@SIDN

SIDN

Thank you for your attention!