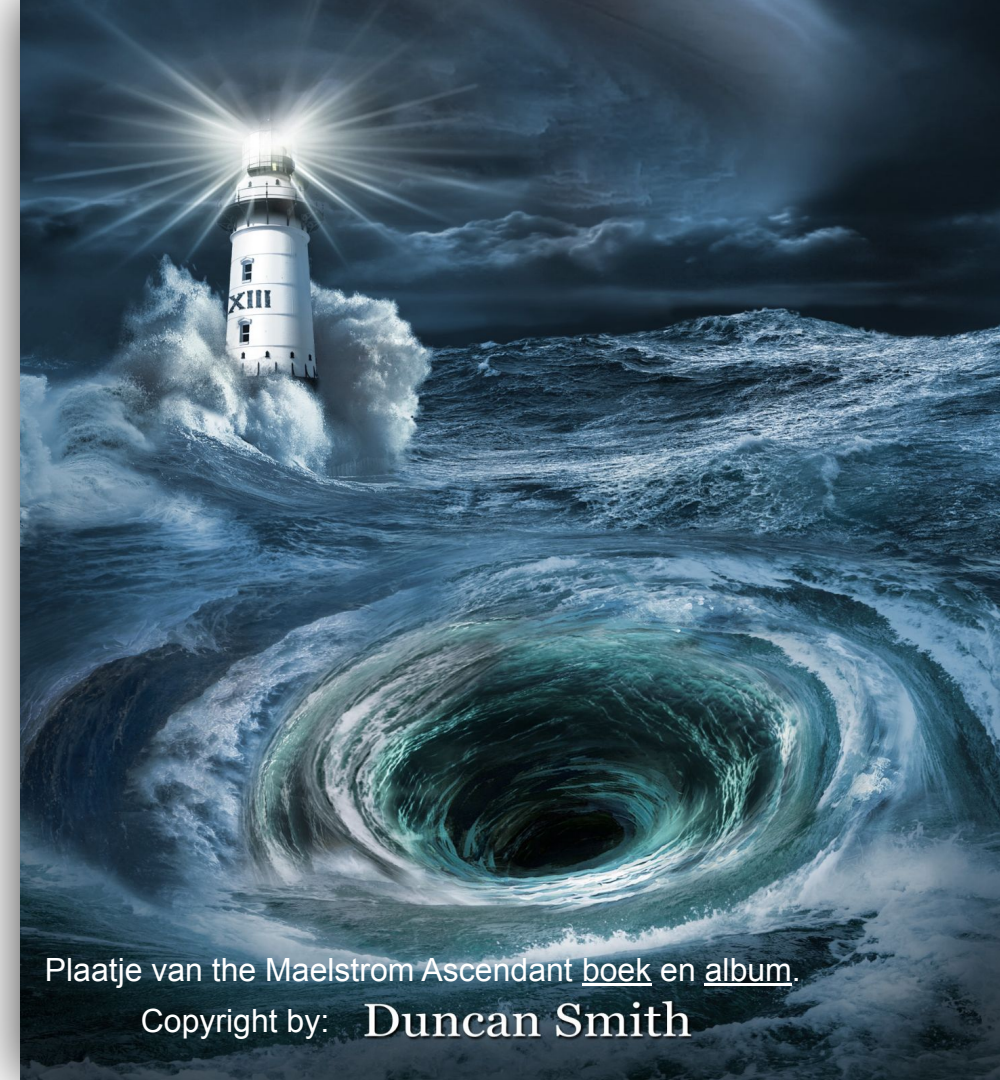
Het opzetten van een Resource Public Key Infrastructure (RPKI) baken

Willem Toorop
NLUUG vj22
10 mei Utrecht



Plaatje van the Maelstrom Ascendant boek en album.
Copyright by: Duncan Smith

Waarom deze presentatie hier

- Het opzetten van het RPKI baken was leuk
  en dat wil ik graag delen
- RPKI is een opkomend security mechanisme voor routeren,
  maar de dynamiek ervan is anders dan TLS en DNSSEC
- Ik wil mijn gedachten hierover graag delen
- Ik wil graag jullie mening en hersens plukken hierover
- Ik wil dat het baken ook nuttig en beschikbaar is voor jullie!

Ontstaan

- Ik werk voor NLnet Labs en werk daar aan DNS software

- Stichting NLnet in 1989 begonnen door de NLUUG
  - Stimuleren van electronic information exchange
  - De eerste internet backbone in Nederland
- NLnet B.V. begint in 1994, Verkocht in 1997
- De stichting ging door
  - Sponsoren van research en software projecten ten behoeve van de internet gemeenschap
- NLnet begint in 1999 stichting NLnet Labs
  - Ontwikkelen van Open Source software en open standaarden ten behoeve van het internet

NLNETLABS

- Non-profit stichting – sinds 1999 – subsidies & donaties

NLNETLABS

- Missie:
  - *Leveren van globaal erkende innovaties en expertise in die technologieën die een netwerk van netwerken maken tot een Open Internet voor allen.*
- Doel:
  - *Ontwikkelen van **Open Source software** en **Open Standaarden** ten behoeve van het Internet,*

    en voorts al hetgeen met één en ander rechtstreeks of zijdelings verband houdt of daartoe bevorderlijk kan zijn, alles in de ruimste zin.

NLNETLABS

- Doel:
  - *Ontwikkelen van **Open Source software** en **Open Standaarden** ten behoeve van het Internet,*

NSD unbound getdns

Open DNSSEC

ROUTINATOR

Krill

- ldns
- Net::DNS
- Net::DNS::SEC

NLNETLABS en nlnet FOUNDATION

- Doel:

> *NLnet Labs writes code,*
> *NLnet writes checks*
>
> *– Michiel Leenaars*

UTINATOR

Krill

- ldns
- Net::DNS
- Net::DNS::SEC

NLNETLABS

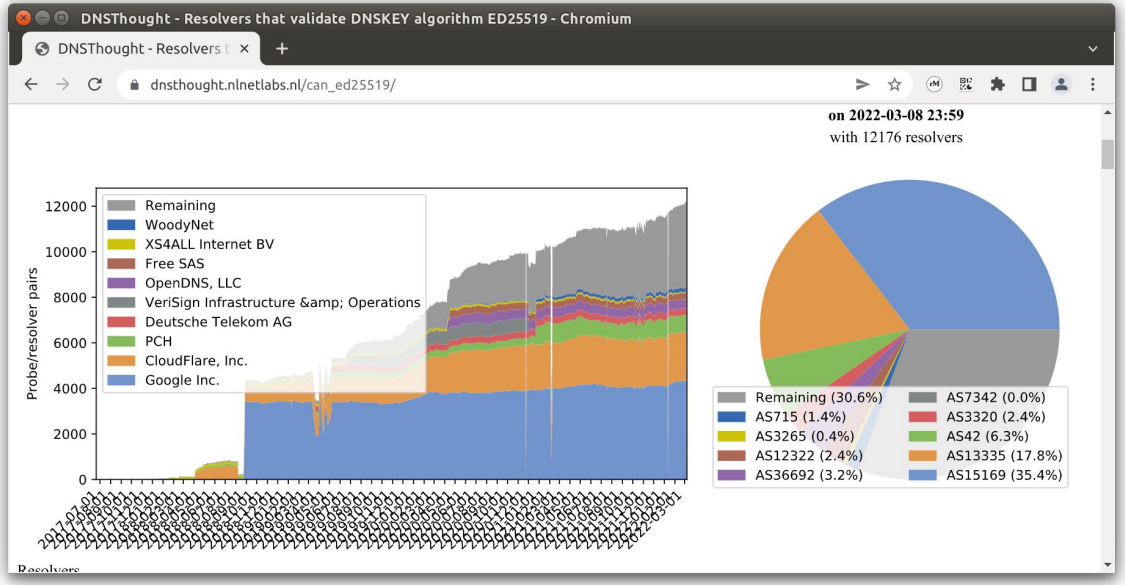
- Doel:
  - *Ontwikkelen van **Open Source software** en **Open Standaarden** ten behoeve van het Internet,*

    en voorts al hetgeen met één en ander rechtstreeks of zijdelings verband houdt of daartoe bevorderlijk kan zijn, alles in de ruimste zin.

Research – Internet metingen – Studenten projecten

Ontstaan

- Ik werk voor NLnet Labs en werk daar aan DNS software
- Ik doe ook metingen van DNS



Onts

- Ik w
- Ik d
- Job
  RPk
  IMC
- Beg
  toer
- Job

ftware

What Happened? The Amazon Route 53 BGP Hijack to Take Over Ethereum Cryptocurrency Wallets | Internet Society - Chromium

What Happened? The Am

internetsociety.org/blog/2018/04/amazons-route-53-bgp-hijack/

Internet Society

Mutually Agreed Norms for Routing Security (MANRS) 27 April 2018

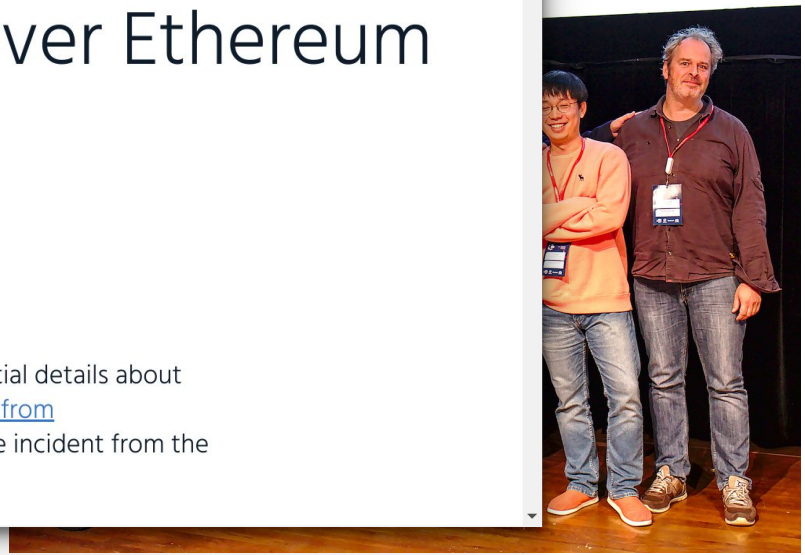
EN ES

What Happened? The Amazon Route 53 BGP Hijack to Take Over Ethereum Cryptocurrency Wallets

By Aftab Siddiqui

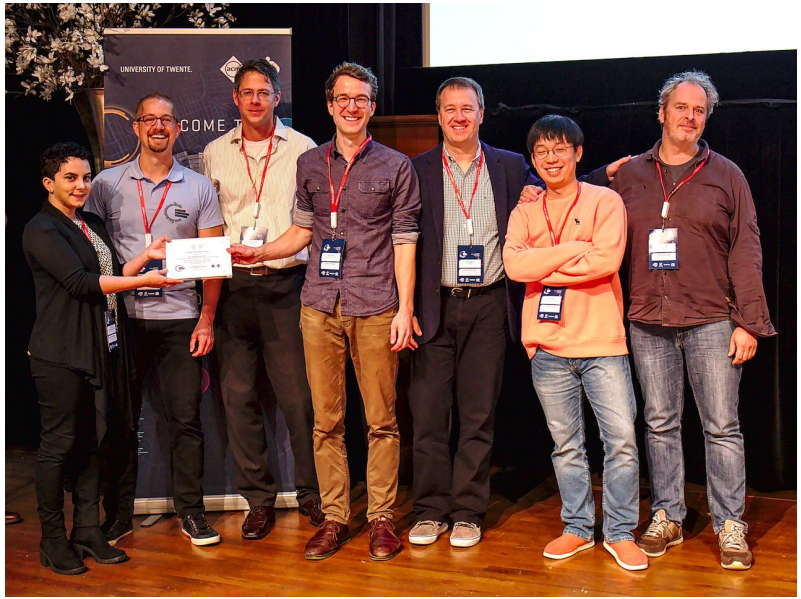
Senior Manager, Internet Technology - Asia-Pacific

Yesterday, we published a blog post sharing the news and some initial details about Amazon's DNS route hijack event to steal Ethereum cryptocurrency from myetherwallet.com. In this post, we'll explore more details about the incident from the BGP hijack's perspective.

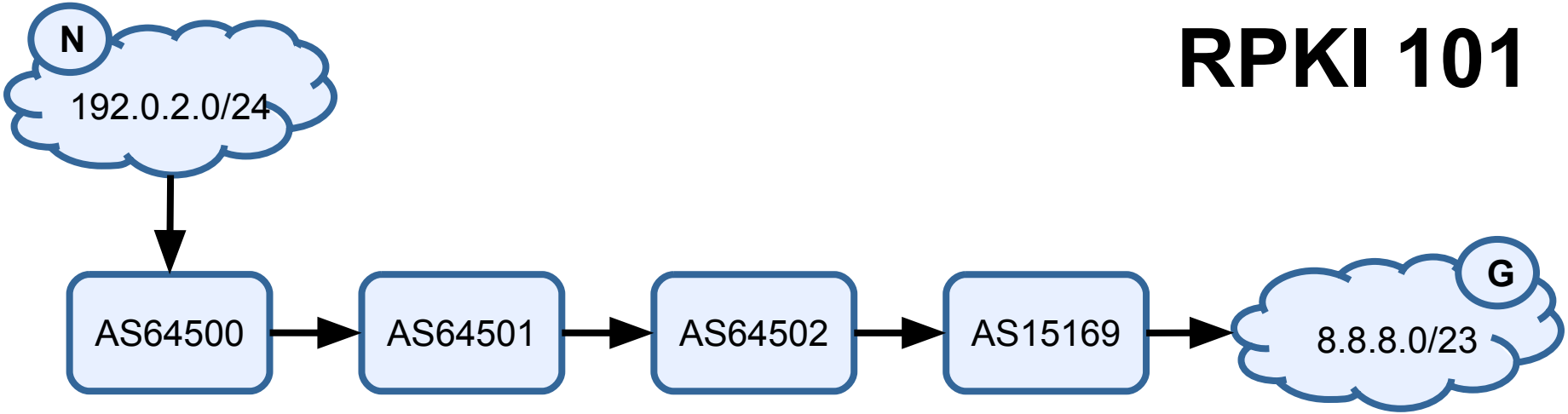


Ontstaan

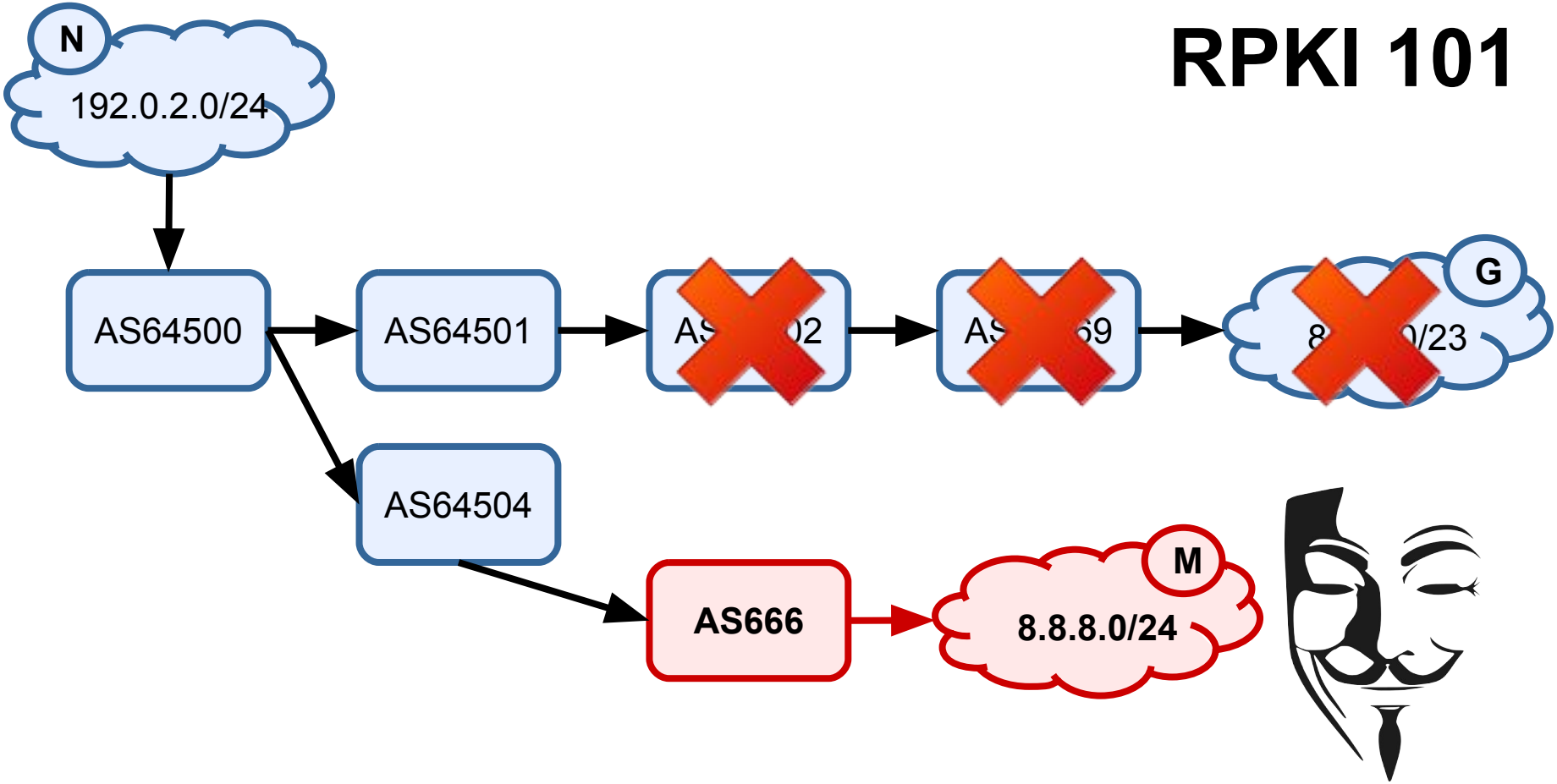
- Ik werk voor NLnet Labs en werk daar aan DNS software
- Ik doe ook metingen van DNS
- Job Snijders bood aan zijn RPKI baken te gebruiken bij IMC2019 in Amsterdam 🙏💖
- Begonnen met het meten van toename sinds januari 2022
- Job's baken EOL in okt. 2020



RPKI 101



RPKI 101



RPKI 101

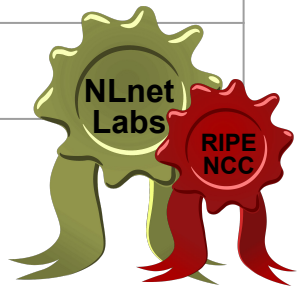
“an infrastructure to support improved security of Internet routing”

RFC6480

Tekenen (Signing)

- Route Origin Authorization

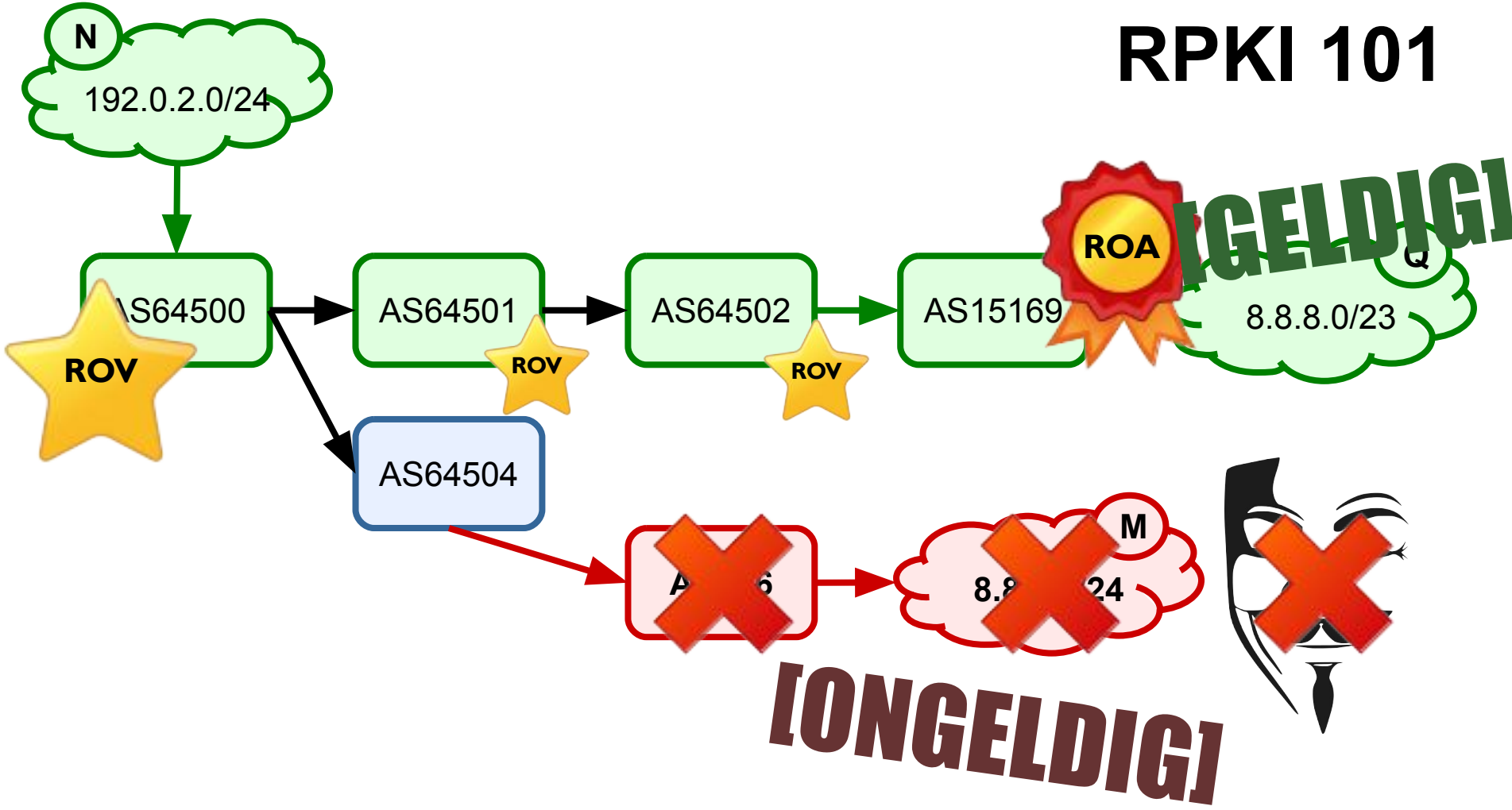
ASN	8587
Prefix	185.49.140.0/23
Max length	23



Validatie

- Route Origin Validation

  Voeg allen prefixes toe met een valide ROA

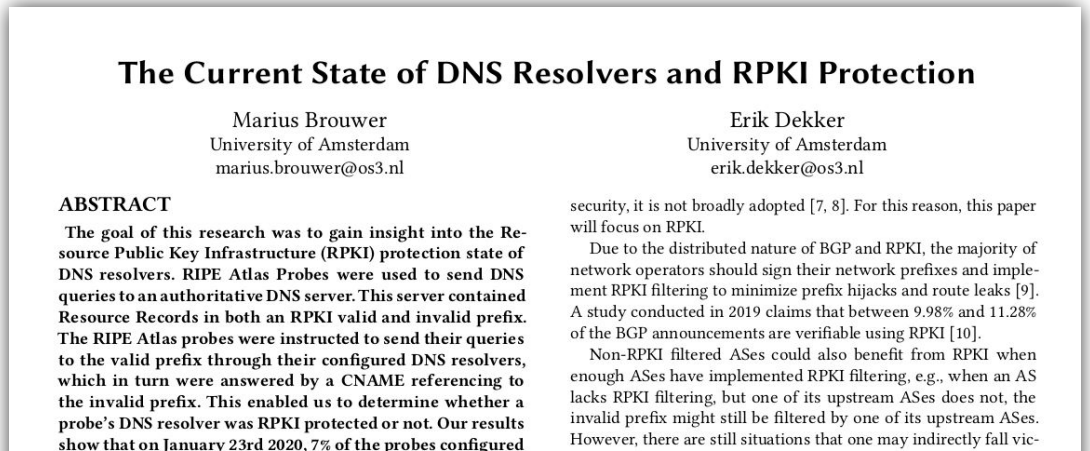

RPKI 101
N
192.0.2.0/24
AS64500
ROV
AS64501
ROV
AS64502
ROV
AS15169
ROA
[GELDIG]
Q
8.8.8.0/23
AS64504
M
[ONGELDIG]

Ontstaan

- Job's RPKI baken (`pete.meerval.net`) in gebruik door
  - RPKI NCC Web test

Ontstaan

- Job's RPKI baken (`pete.meerval.net`) in gebruik door
  - RPKI NCC Web test
  - DNS-OARC's Check my DNS
  - Research project met Security en Network Engineering



The Current State of DNS Resolvers and RPKI Protection

Marius Brouwer
University of Amsterdam
marius.brouwer@os3.nl

Erik Dekker
University of Amsterdam
erik.dekker@os3.nl

ABSTRACT

The goal of this research was to gain insight into the Resource Public Key Infrastructure (RPKI) protection state of DNS resolvers. RIPE Atlas Probes were used to send DNS queries to an authoritative DNS server. This server contained Resource Records in both an RPKI valid and invalid prefix. The RIPE Atlas probes were instructed to send their queries to the valid prefix through their configured DNS resolvers, which in turn were answered by a CNAME referencing to the invalid prefix. This enabled us to determine whether a probe's DNS resolver was RPKI protected or not. Our results show that on January 23rd 2020, 7% of the probes configured

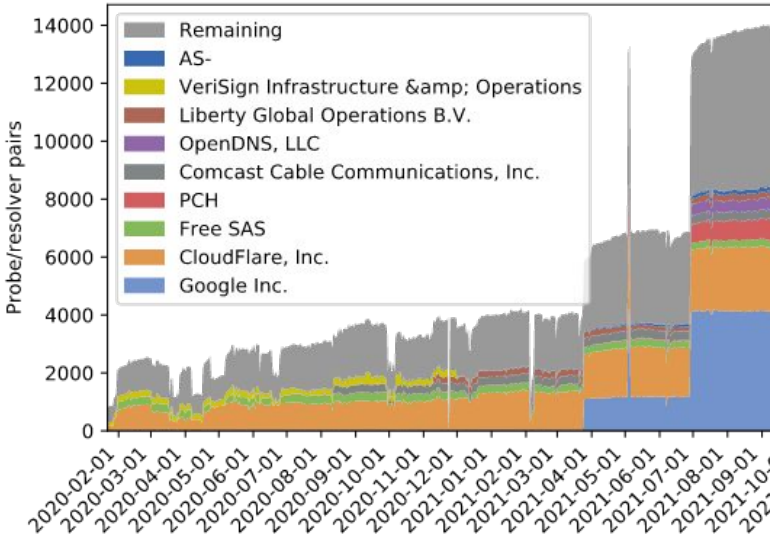
security, it is not broadly adopted [7, 8]. For this reason, this paper will focus on RPKI.

Due to the distributed nature of BGP and RPKI, the majority of network operators should sign their network prefixes and implement RPKI filtering to minimize prefix hijacks and route leaks [9]. A study conducted in 2019 claims that between 9.98% and 11.28% of the BGP announcements are verifiable using RPKI [10].

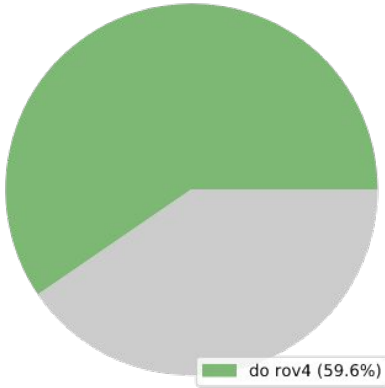
Non-RPKI filtered ASes could also benefit from RPKI when enough ASes have implemented RPKI filtering, e.g., when an AS lacks RPKI filtering, but one of its upstream ASes does not, the invalid prefix might still be filtered by one of its upstream ASes. However, there are still situations that one may indirectly fall vic-

Ontstaan

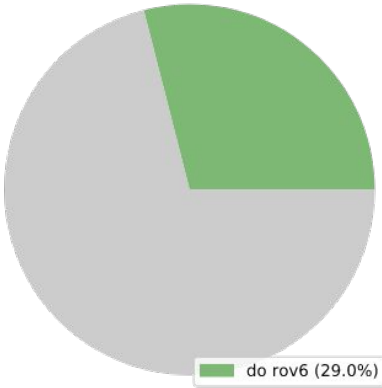
- Job's RPKI baken (`pete.meerval.net`) in gebruik door
  - RPKI NCC Web test
  - DNS-OARC's Check my DNS



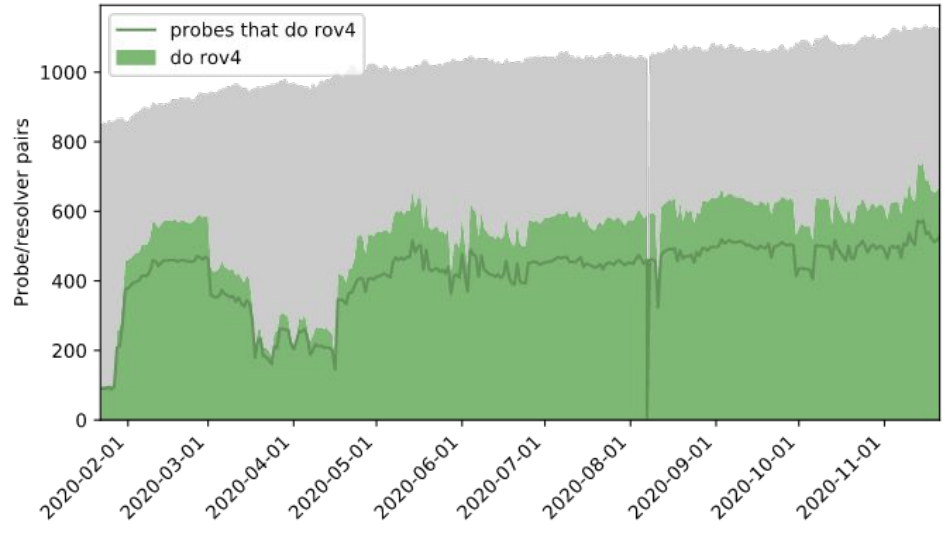
RoV van Cloudflare resolvers (AS13335)

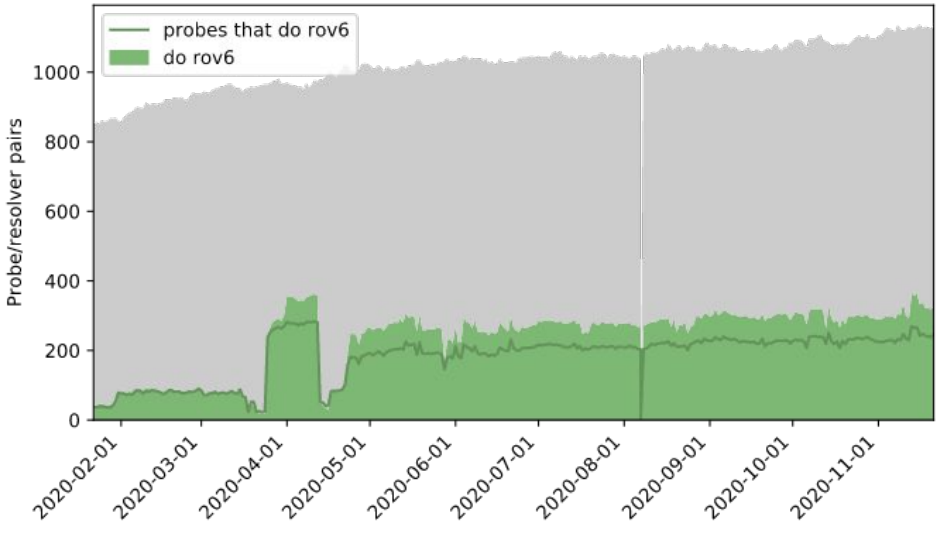


IPv4



IPv6





RoV van Cloudflare resolvers (AS13335)

Re: rov for cloudflare quad-1 resolver - Postvak IN - willem@nlnetlabs.nl - Mozill

Postvak IN - willem@nlnetlabs. | Re: rov for cloudflare quad-

Doorsturen | Archiveren | Ongewenst | Verwijderen | Meer

Van Louis Poinsignon <louis@cloudflare.com>

Onderwerp **Re: rov for cloudflare quad-1 resolver** 04-02-2020 16:39

Aan Martin J. Levy <martin@cloudflare.com>

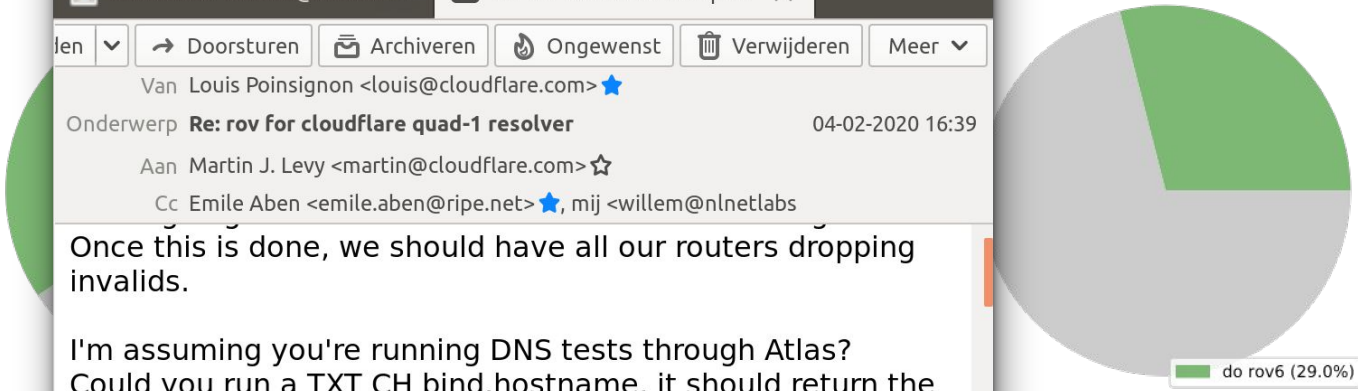
Cc Emile Aben <emile.aben@ripe.net>, mij <willem@nlnetlabs

Once this is done, we should have all our routers dropping invalids.

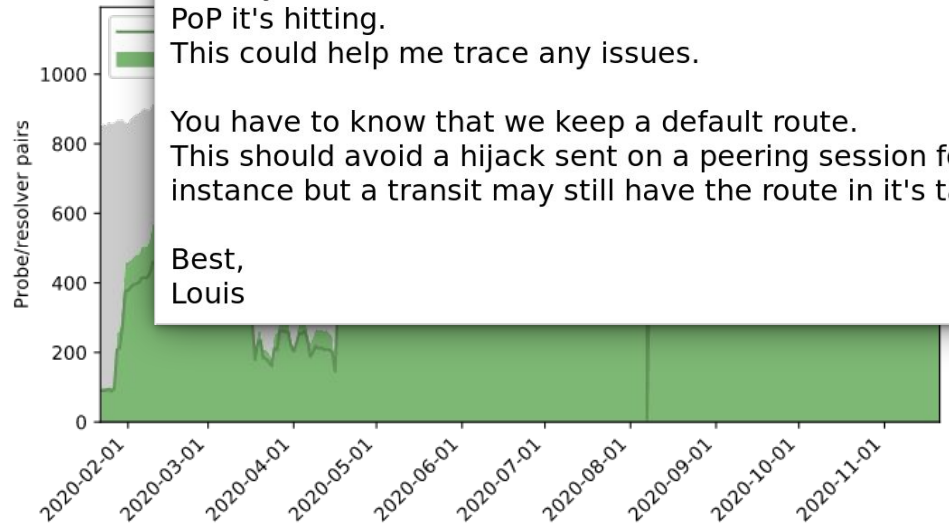
I'm assuming you're running DNS tests through Atlas?
Could you run a TXT CH bind.hostname, it should return the PoP it's hitting.
This could help me trace any issues.

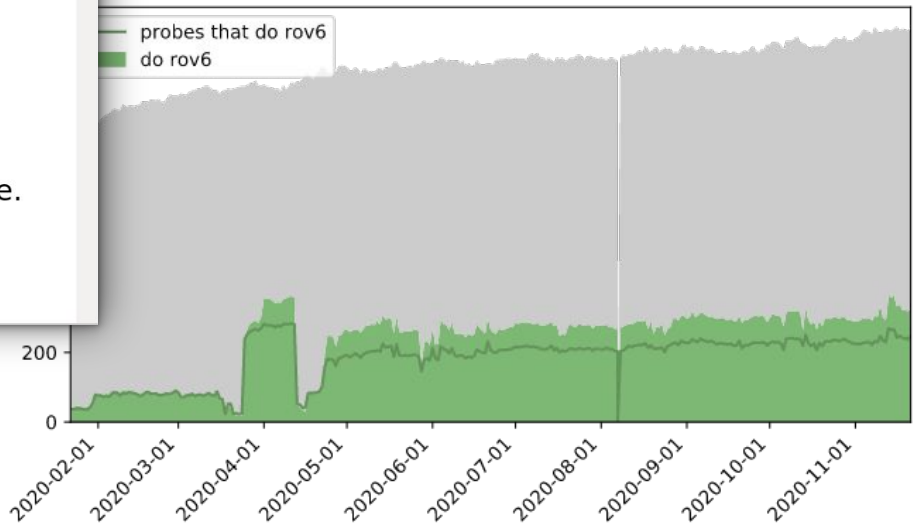
You have to know that we keep a default route.
This should avoid a hijack sent on a peering session for instance but a transit may still have the route in it's table.

Best,
Louis



IPv6





RoV van Cloudflare resolvers (AS13335)

Re: rov for cloudflare quad-1 resolver - Postvak IN - willem@nlnetlabs.nl - Mozill

Postvak IN - willem@nlnetlabs.

Re: rov for cloudflare quad-

Doorsturen | Archiveren | Ongewenst | Verwijderen | Meer

Van Louis Poinsignon <louis@cloudflare.com>

Onderwerp

Once t
invalids

I'm ass
Could y
PoP it's
This co

You hav
This sh
instanc

Best,
Louis

Re: rov for cloudflare quad-1 resolver - Postvak IN - willem@nlnetlabs.nl - Mozilla Thunde

Postvak IN - willem@nlnetlabs.

Re: rov for cloudflare quad-

Beantwoorden | Doorsturen | Archiveren | Ongewenst | Verwijderen | Meer

Van Martin J. Levy <martin@cloudflare.com>

Onderwerp **Re: rov for cloudflare quad-1 resolver** 04-02-2020 16:44

Aan Louis Poinsignon <louis@cloudflare.com>

Cc Emile Aben <emile.aben@ripe.net> mij <w

Louis,

Let's make that: `TXT CH id.server` a

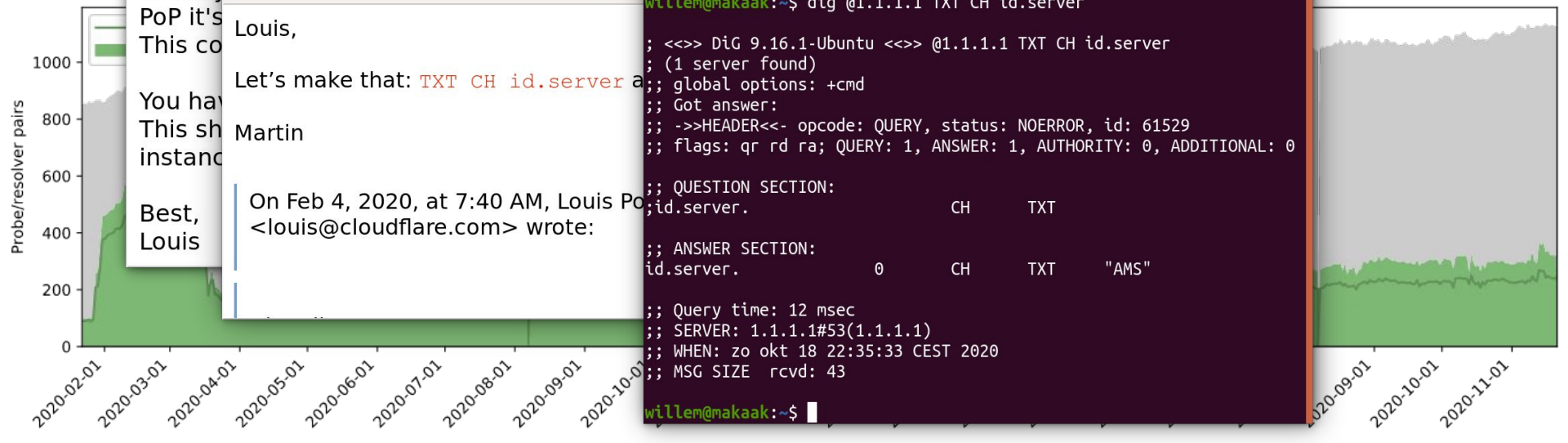
Martin

> On Feb 4, 2020, at 7:40 AM, Louis Po
> <louis@cloudflare.com> wrote:

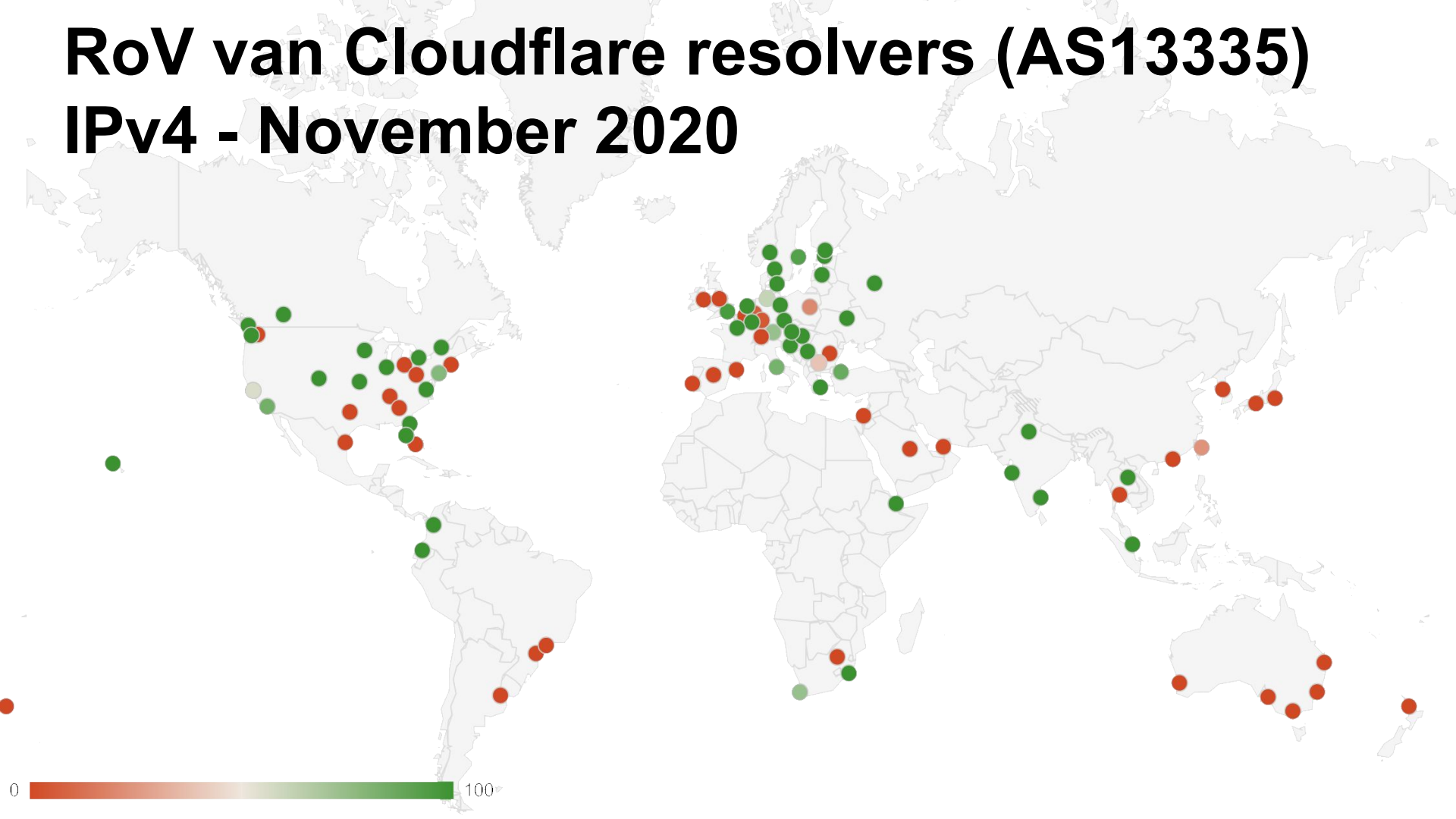
willem@makaak: ~

```
willem@makaak:~$ dig @1.1.1.1 TXT CH id.server

; <<>> DiG 9.16.1-Ubuntu <<>> @1.1.1.1 TXT CH id.server
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61529
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;id.server.                     CH      TXT

;; ANSWER SECTION:
id.server.              0       CH      TXT     "AMS"

;; Query time: 12 msec
;; SERVER: 1.1.1.1#53(1.1.1.1)
;; WHEN: zo okt 18 22:35:33 CEST 2020
;; MSG SIZE  rcvd: 43

willem@makaak:~$
```

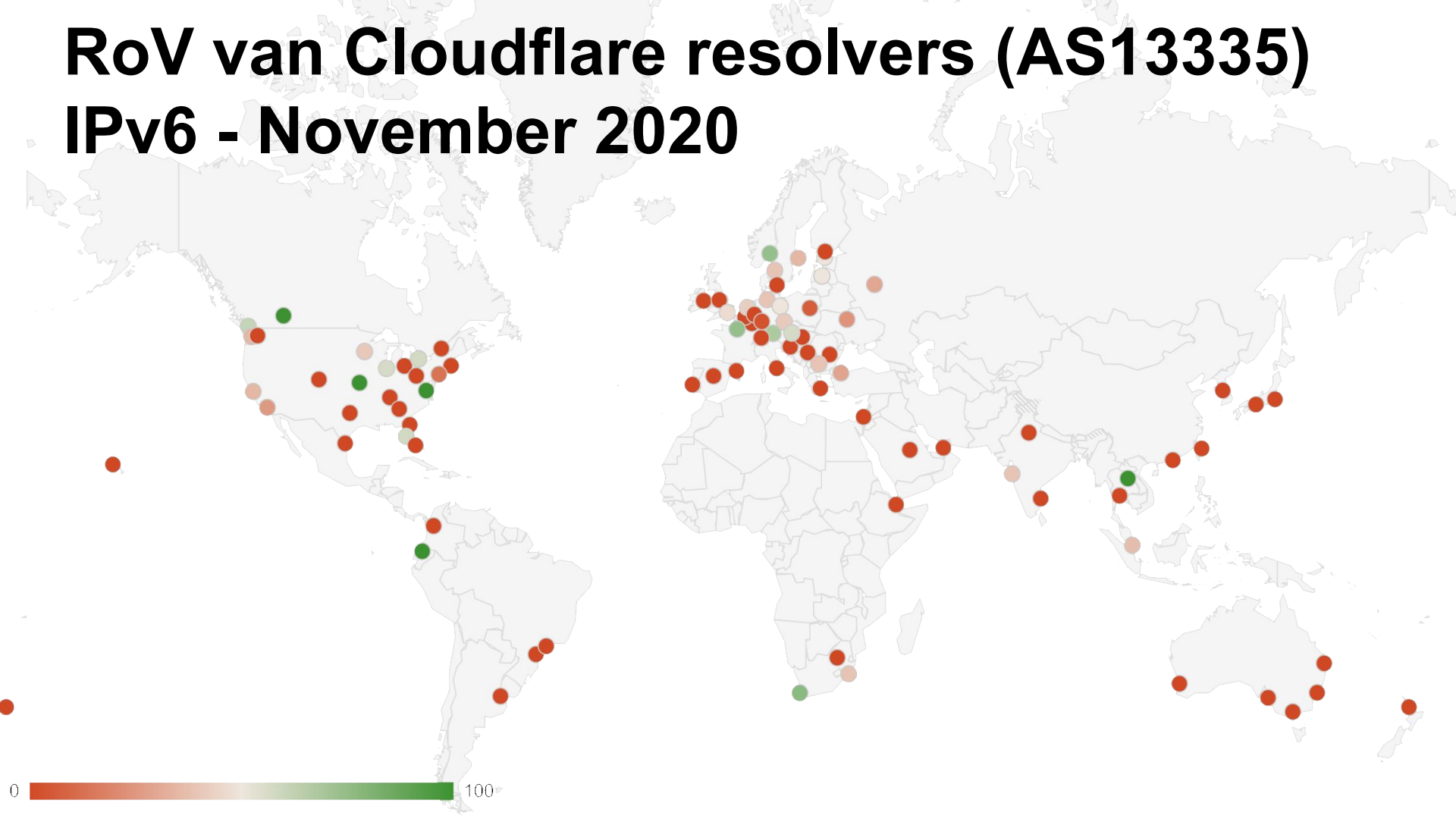
IPv6



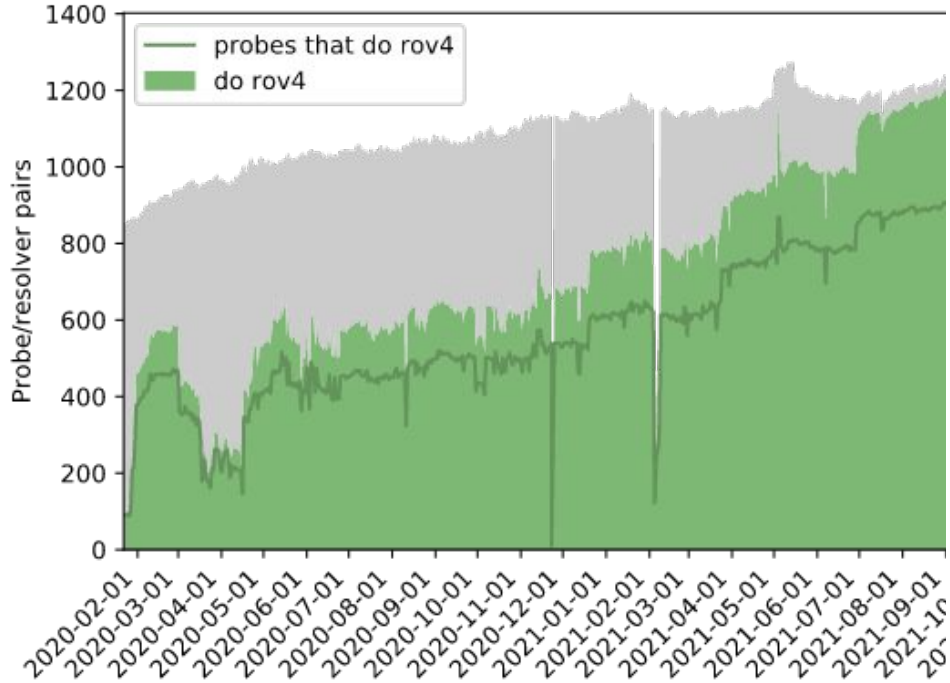
RoV van Cloudflare resolvers (AS13335) IPv4 - November 2020

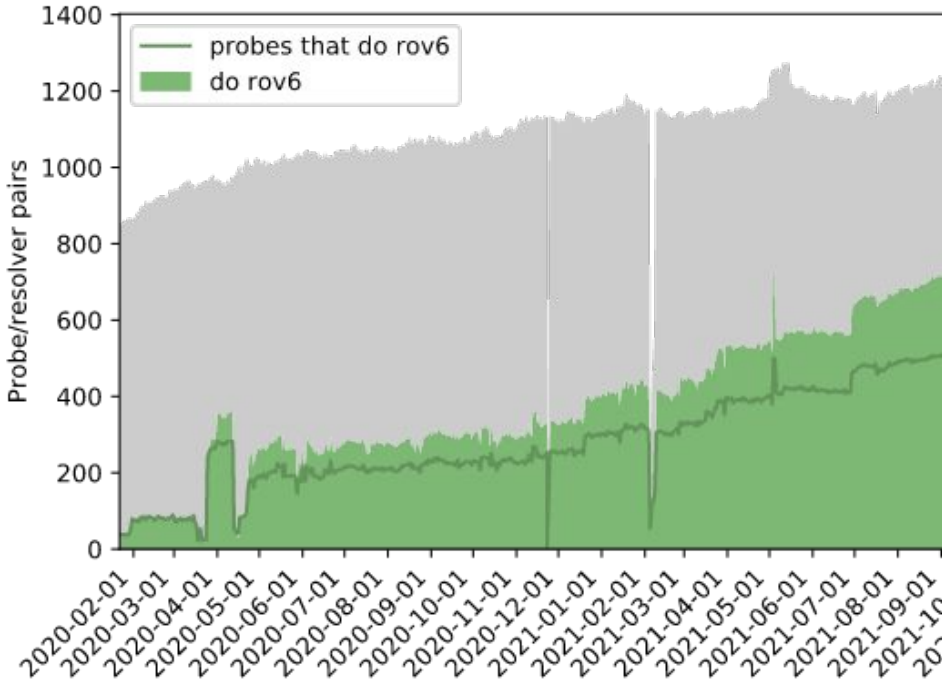


RoV van Cloudflare resolvers (AS13335) IPv6 - November 2020



RoV van Cloudflare resolvers (AS13335) September 2021





Ontstaan

- Job's RPKI baken (`pete.meerval.net`) in gebruik door
  - RPKI NCC Web test
  - DNS-OARC's Check my DNS
  - DNSThought

- October 2020
  - Gevraagd uit te kijken naar een ander RPKI baken

Herevaluatie baken - voorheen

- Ongeldige IPv4 /24 & IPv6 /48 (+ geldige ter referentie)

✔ Als de eerste hop valideert → ongeldig = onbereikbaar

✗ Als een hop op het pad valideert → ongeldig = onbereikbaar

✗ De validerende hop kan in het pad terug voorkomen

Herevaluatie baken - voorheen

```
$ORIGIN rootcanary.net
$TTL 60
@       SOA     ns1.surfnet.nl. (
                dns-beheer.surfnet.nl.
                2020080503 ; serial
                10800      ; refresh
                3600       ; retry
                604800     ; expire
                86400      ; minimum
                )
        NS      ns1.surfnet.nl.
        NS      ns2.surfnet.nl.
        NS      ns3.surfnet.nl.
        NS      ns1.zurich.surf.net.

$TTL 25200

valid4 NS       valid4
valid4 A        209.24.1.6

invalid4        NS      invalid4
invalid4        A       194.32.71.6
```

```
$ORIGIN valid4.rootcanary.net
$TTL 300
@               SOA     valid4.rootcanary.net. (
                        sysadm.rootcanary.org.
                        2020012100 10800 3600
                        604800 300 )
                NS      @
                A       209.24.1.6
$TTL 1
invalid         DNAME invalid4.rootcanary.net.
```

prefix	209.24.1.0/24
max len	24
ASN	15562

ROA

[GELDIG]

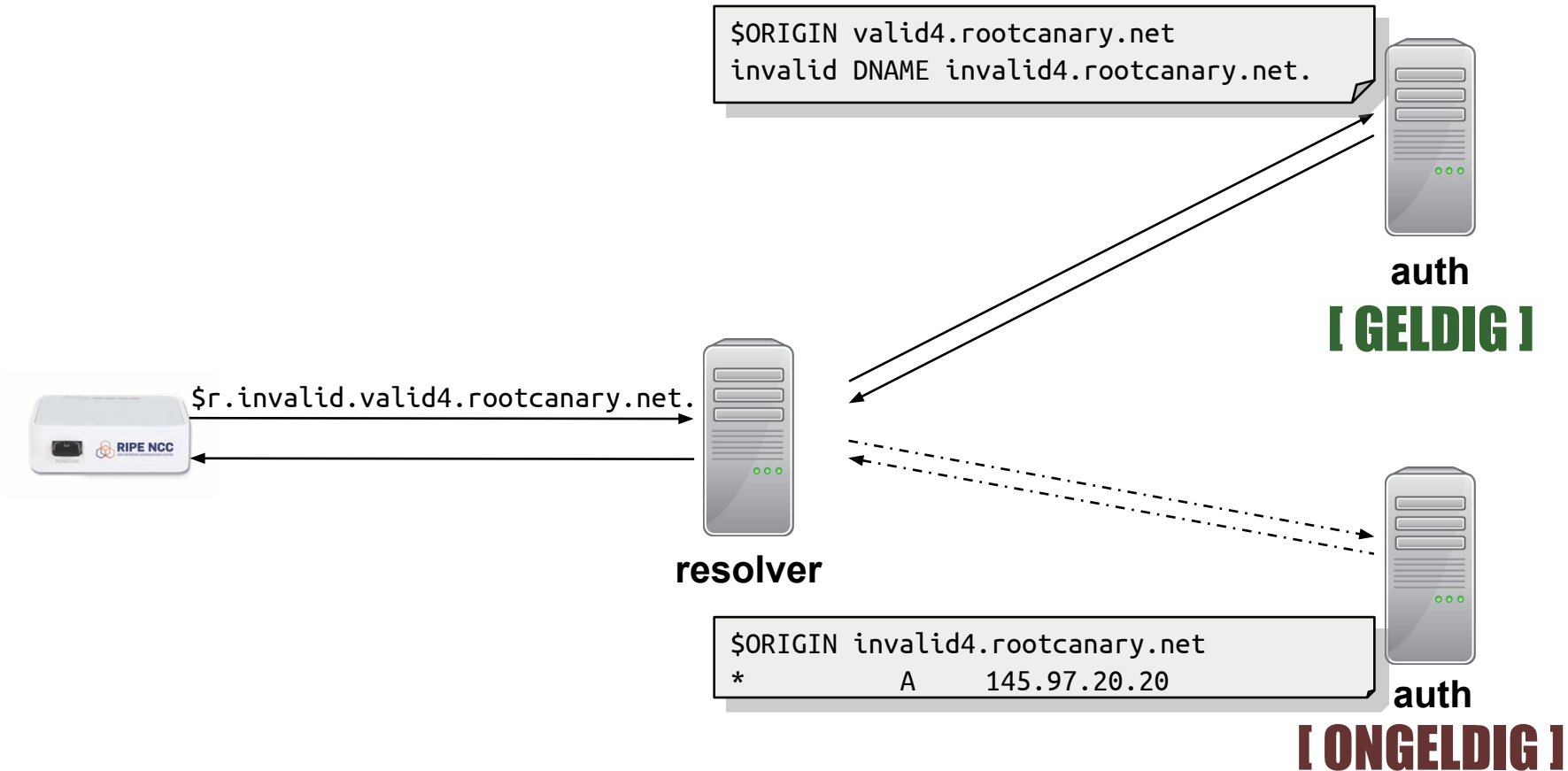
```
$ORIGIN invalid4.rootcanary.net
$TTL 300
@               SOA     invalid4.rootcanary.net. (
                        sysadm.rootcanary.org.
                        2020012100 10800 3600
                        604800 300 )
                NS      @
                A       194.32.71.6
*               A       145.97.20.20
```

prefix	194.32.71.0/24
max len	24
ASN	0

ROA

[ONGELDIG]

Herevaluatie baken - voorheen



Herevaluatie baken - voorheen

- Ongeldige IPv4 /24 & IPv6 /48 (+ geldige ter referentie)

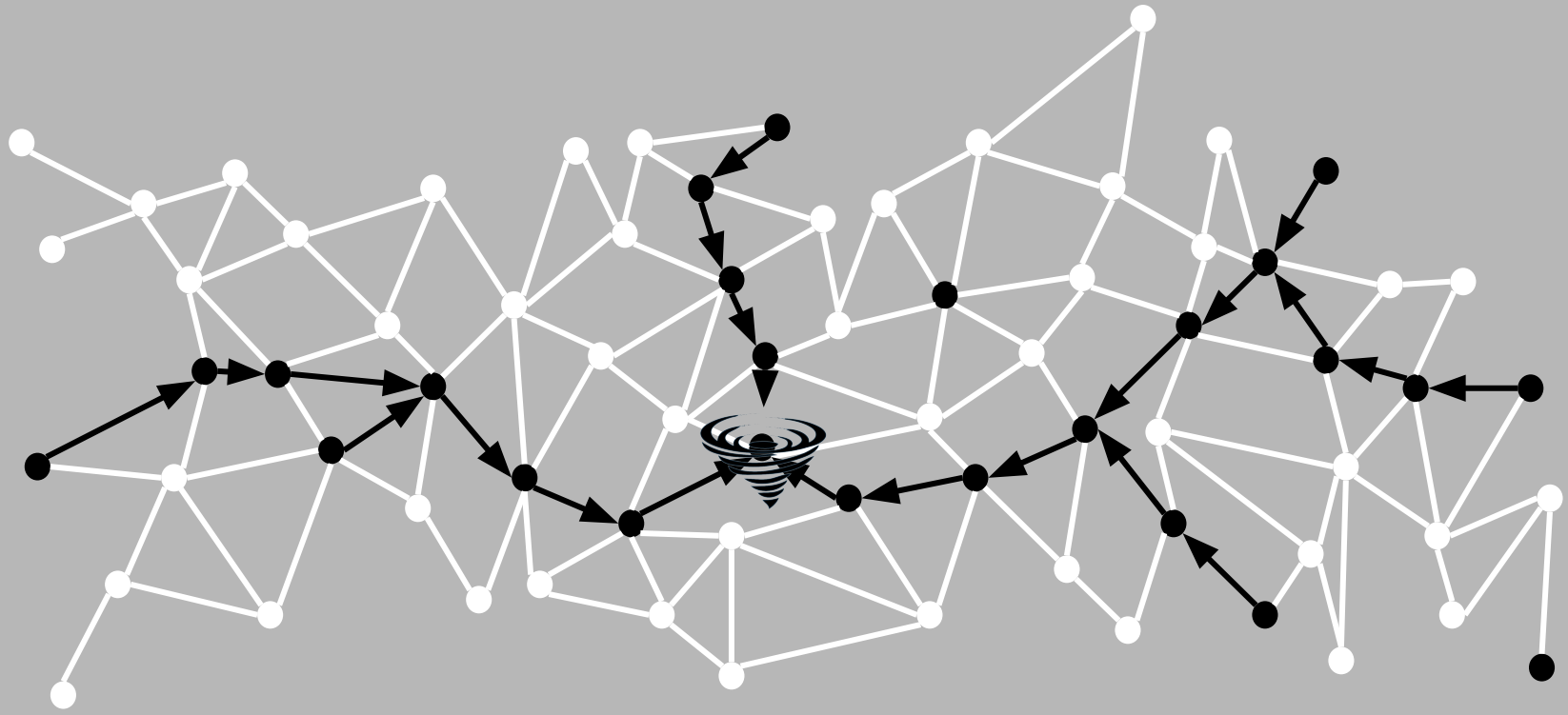
✔ Als de eerste hop valideert → ongeldig = onbereikbaar

✗ Als een hop op het pad valideert → ongeldig = onbereikbaar

✗ De validerende hop kan in het pad terug voorkomen

✗ Detectie gebaseerd op onbereikbaarheid (timeout)

Herevaluatie baken - voorheen



Herevaluatie baken - voorheen

- Ongeldige IPv4 /24 & IPv6 /48 (+ geldige ter referentie)

✔ Als de eerste hop valideert → ongeldig = onbereikbaar

✗ Als een hop op het pad valideert → ongeldig = onbereikbaar

✗ De validerende hop kan in het pad terug voorkomen

✗ Detectie gebaseerd op onbereikbaarheid (timeout)

✗ Is dit een realistische routing hijack?

Herevaluatie baken - nieuwe setup

- Geldig /23 (IPv4) en /47 (IPv6) en Ongeldig /24 en /48 more specific announcements van elders
  - ✔ Een meer realistische route hijack?
  - ✔ Geen detectie gebaseerd op onbereikbaarheid (geen timeouts)

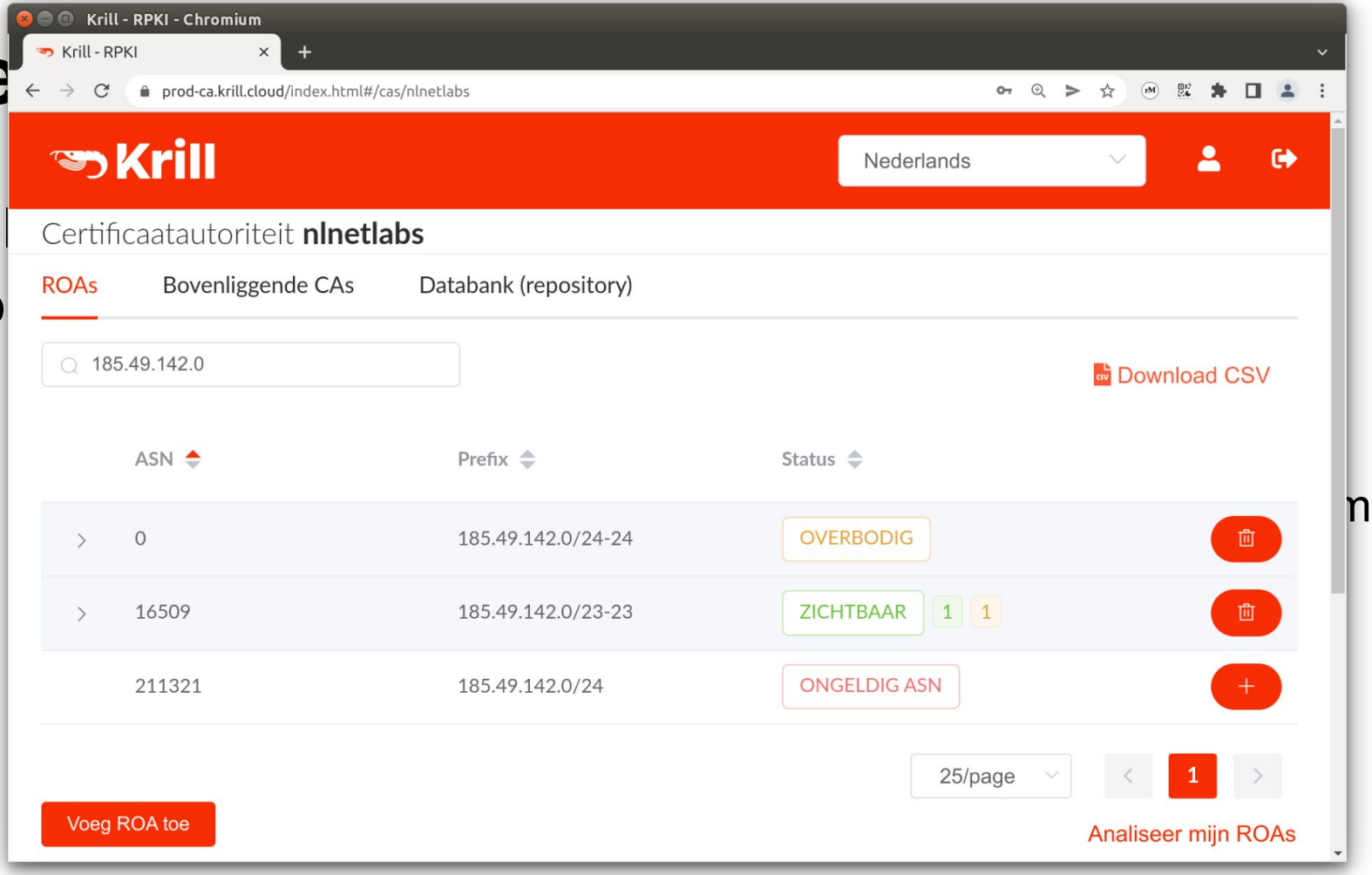
He

- Ge
mo

✔

✔

meouts)



Herevaluatie baken - nieuwe setup

- Geldig /23 (IPv4) en /47 (IPv6) en Ongeldig /24 en /48 more specific announcements van elders

✔ Een meer realistische route hijack?

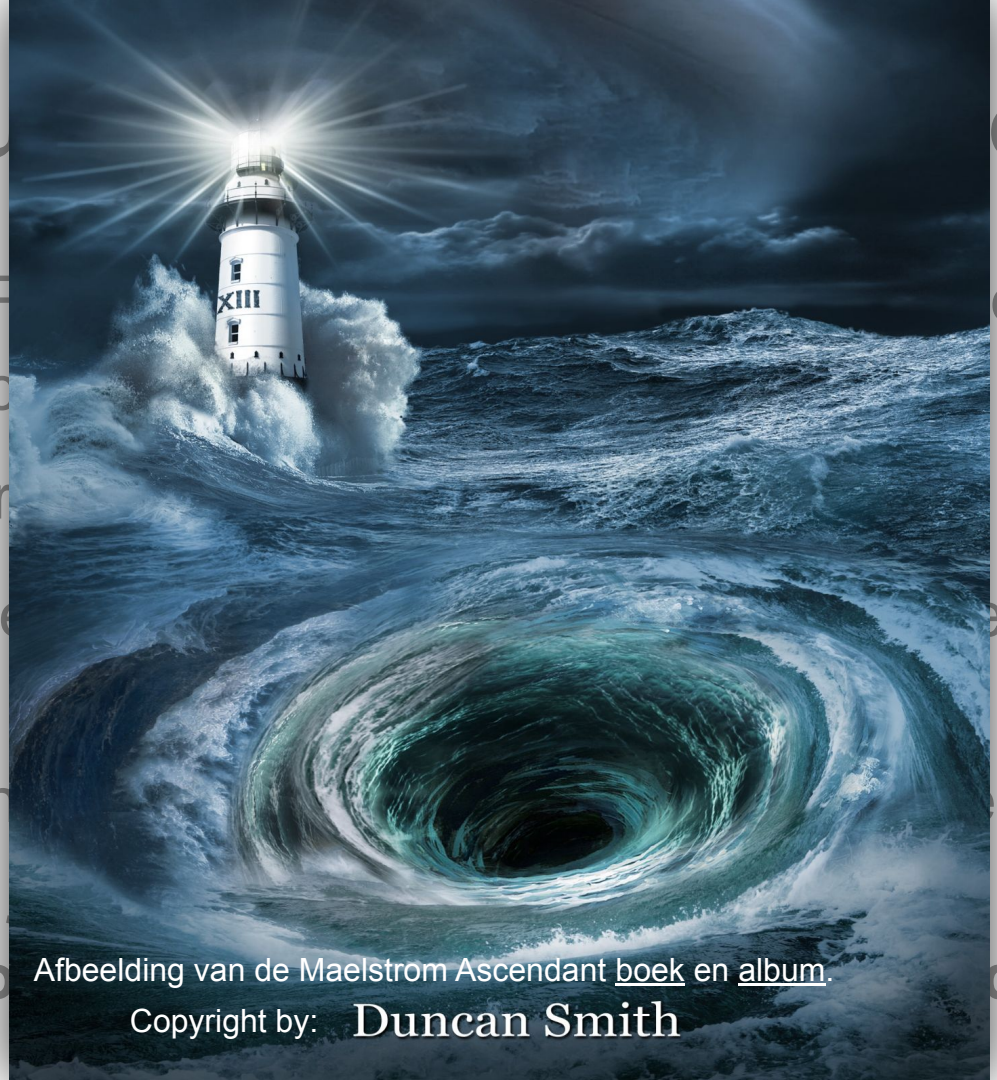
✔ Geen detectie gebaseerd op onbereikbaarheid (geen timeouts)

✗ We weten nog steeds niet welke hop valideert

✗ **Zelfs als jouw network valideert, kun je nog steeds bij de ongeldige (invalid) uitkomen!**

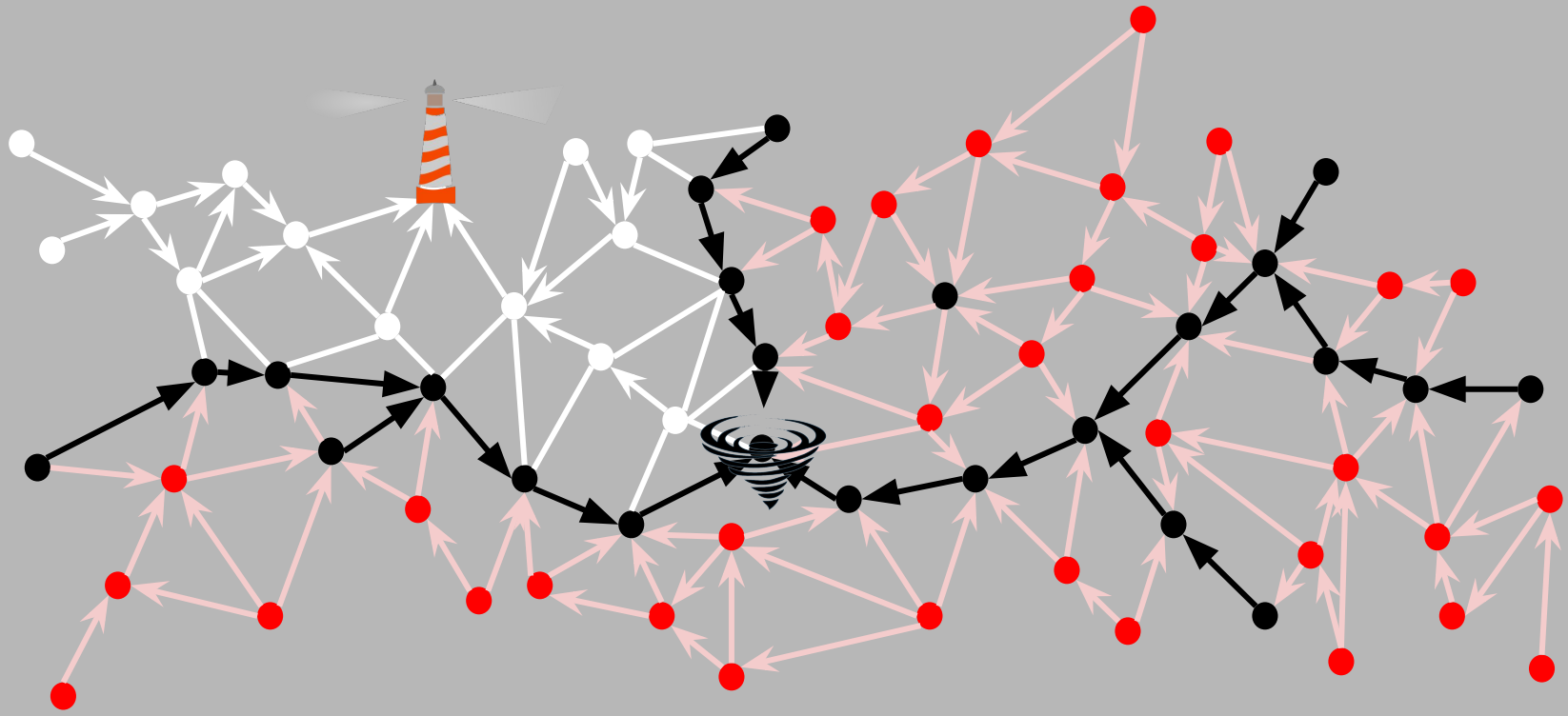
Herevalu etup

- Geldig /23 (IF en /48 more specific
  - ✔ Een meer
  - ✔ Geen dete eid (geen timeouts)
  - ✗ We weten rt
  - ✗ **Zelfs als kun je no d) uitkomen!**

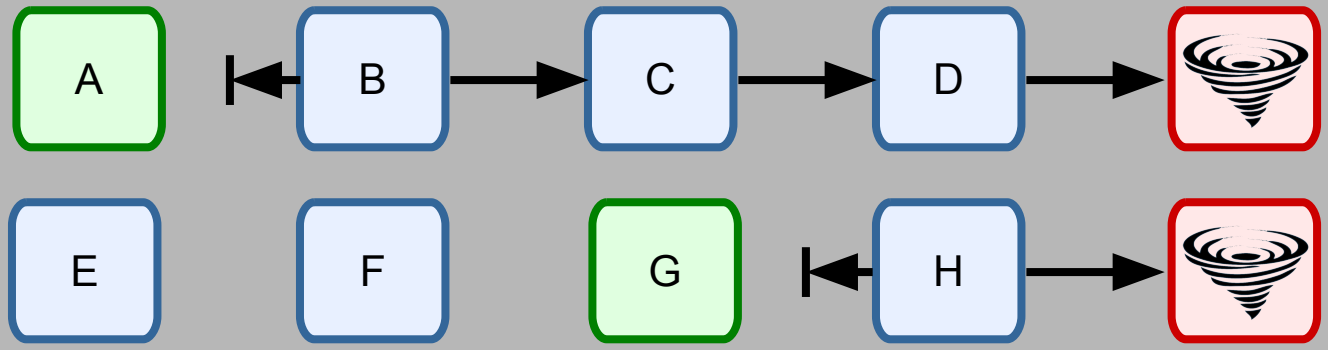


Afbeelding van de Maelstrom Ascendant boek en album.
Copyright by: Duncan Smith

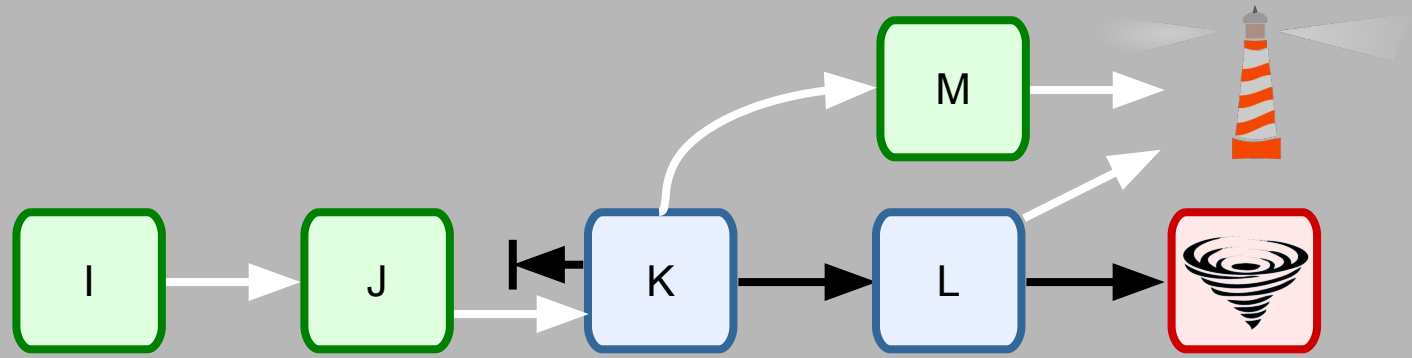
Herevaluatie baken - nieuwe setup



Herevaluatie baken - voorheen



Herevaluatie baken - nieuwe setup



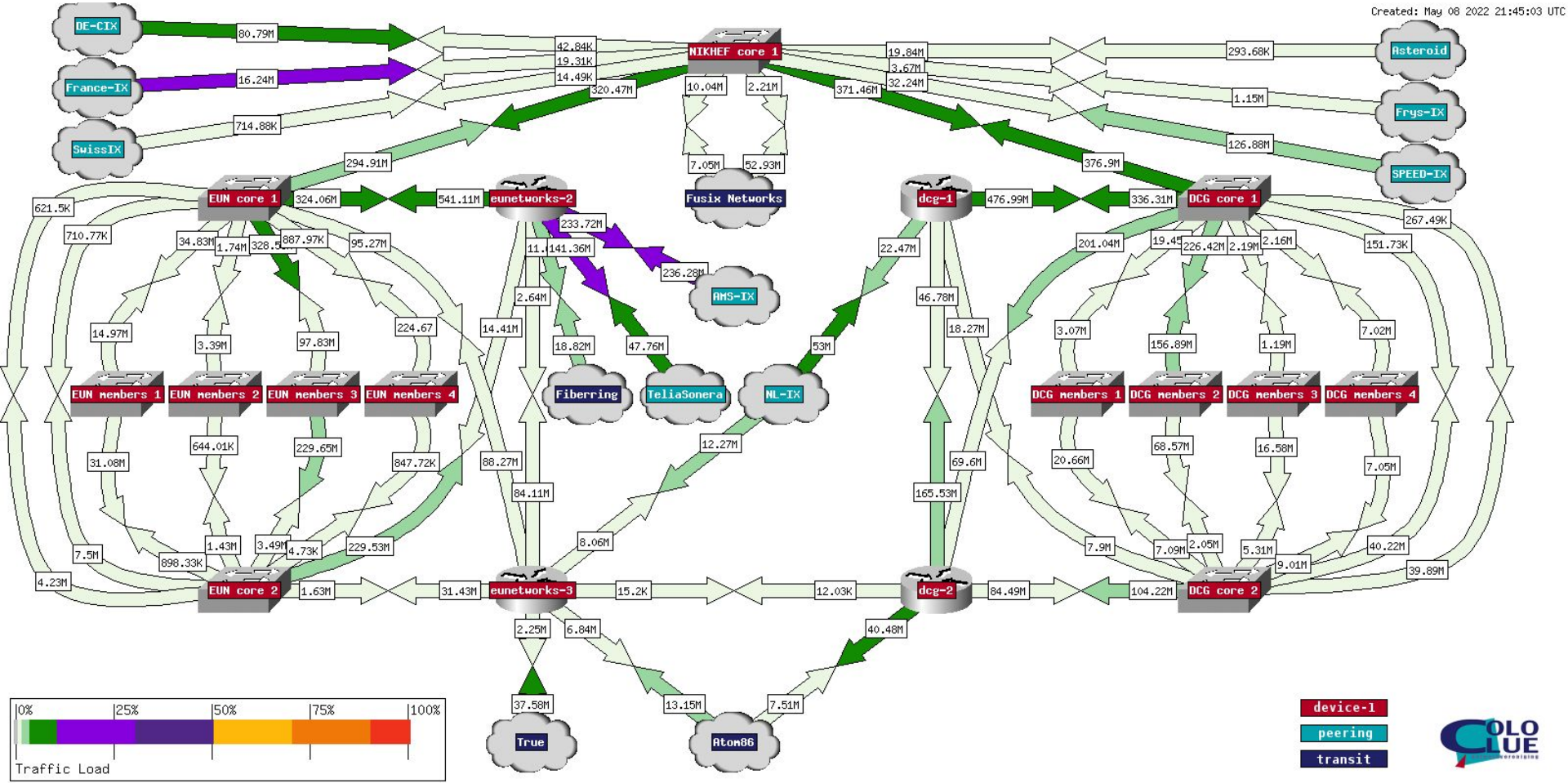
Ontstaan

- december 2020 Resources aangevraagd bij RIPE NCC
- januari 2021 Tijdelijke resources gekregen (1 jaar)
  - Less specific /23 en /47 announced via AWS
  - More specific /24 en /48 via de University Twente
  - Zonder succes…
- juni 2021
  - De less specific verhuisd naar Coloclue!
  - Succes!!!

O

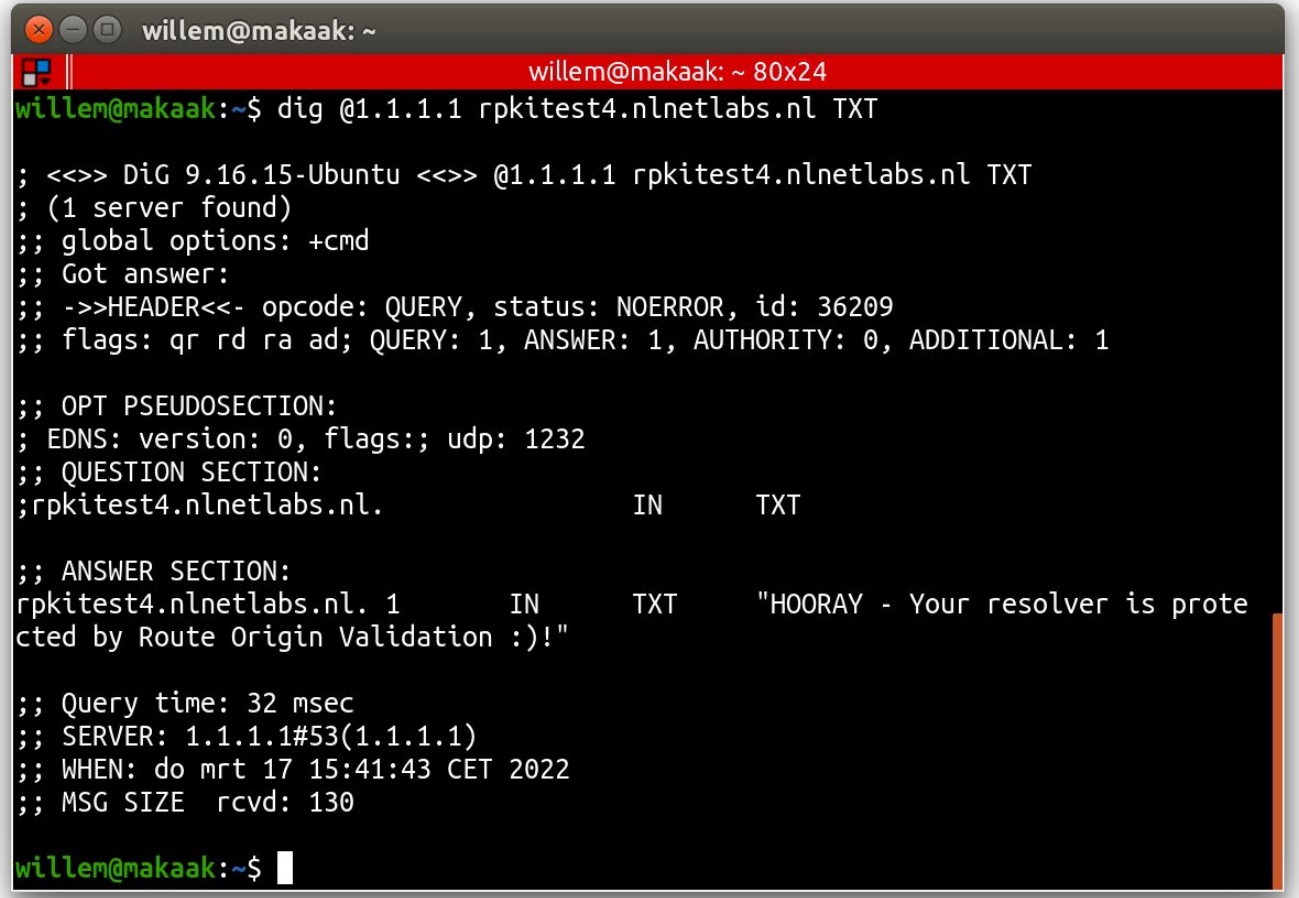
-
-
-


ColoClue – Welkom bij Netwerkvereniging ColoClue - Chromium
ColoClue – Welkom bij Ne
coloclue.net
Netwerk
Nieuws
Kosten
FAQ
Site map
Aanmelden
Contact
Nederlands
Netwerkvereniging ColoClue
Colocatie waarbij JIJ het voor het zeggen hebt!
Netwerkvereniging ColoClue is een vereniging, zonder winstoogmerk, als hobbyproject en in vrije tijd opgezet door medewerkers van enkele Internet-providers. We hebben een volledig onafhankelijk, eigen netwerk, AS8283, dat verbonden is met diverse transitproviders.
CLUEMETER
April 2022
Racks : 8
Machines : 127
Leden : 191


Created: May 08 2022 21:45:03 UTC
DE-CIX
France-IX
SwissIX
NIKHEF core 1
Asteroid
Frys-IX
SPEED-IX
EUN core 1
eunetworks-2
Fusix Networks
dcg-1
DCG core 1
AMS-IX
Fiberring
TeliaSonera
NL-IX
EUN members 1
EUN members 2
EUN members 3
EUN members 4
DCG members 1
DCG members 2
DCG members 3
DCG members 4
EUN core 2
eunetworks-3
dcg-2
DCG core 2
True
Atom86
0%
25%
50%
75%
100%
Traffic Load
device-1
peering
transit

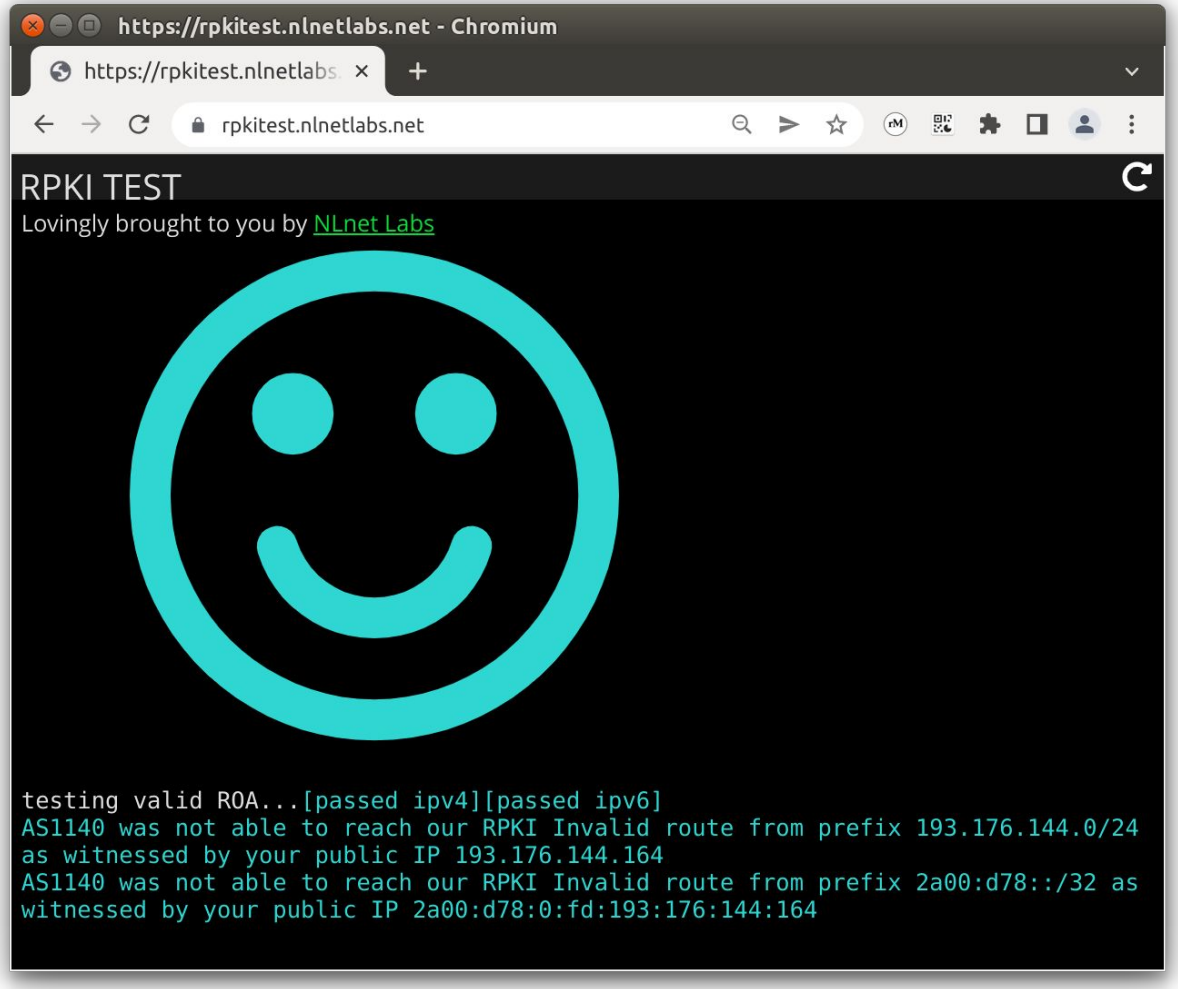
Tools

- Resolver test: onmiddellijk resultaat! 👍



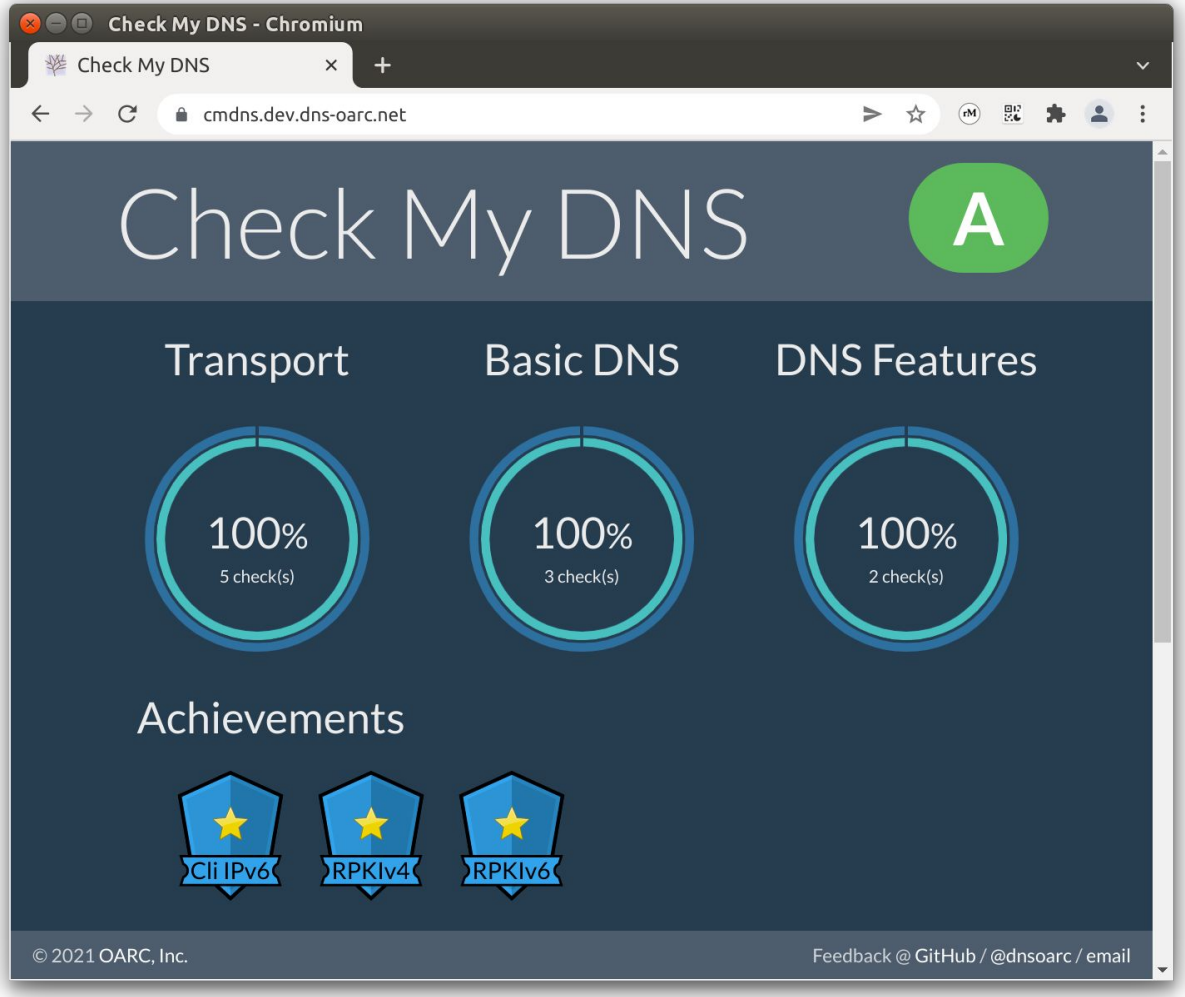
Tools

- Resolver test: onmiddellijk resultaat! 👍
- Web test: onmiddellijk resultaat! 👍



Tools

- Resolver test: onmiddellijk resultaat! 👍
- Web test
- DNS OARC's Check My DNS RPKI Test 👍

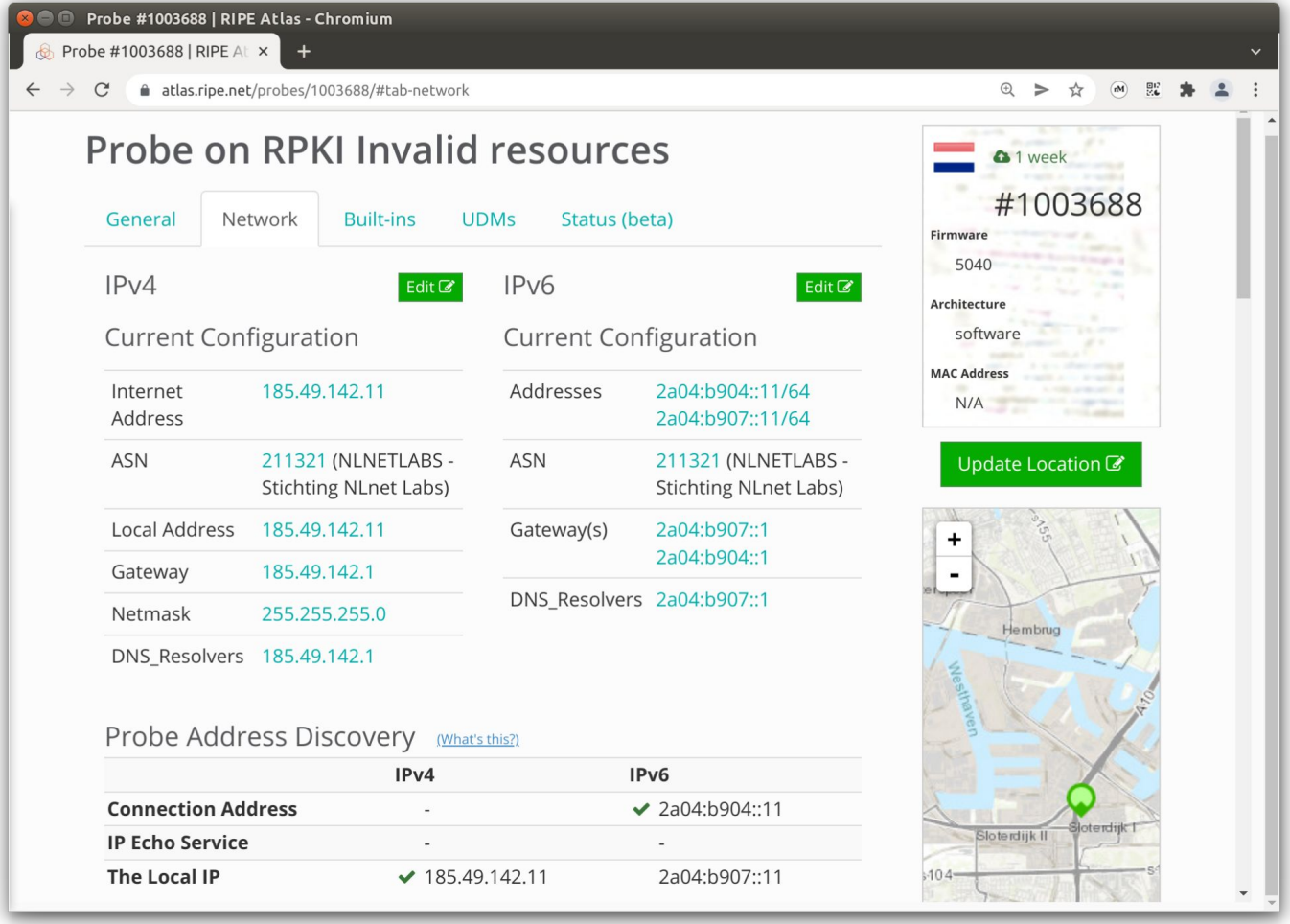


Ontstaan

- januari 2022 — Tijdelijke resource verlopen
  Verhuisd naar onze eigen IPv4 resources
  (moest ik eerst vrijmaken)
- februari 2022 — DIY MSMs: NLNOG Ring / RIPE Atlas

DIY MSMs

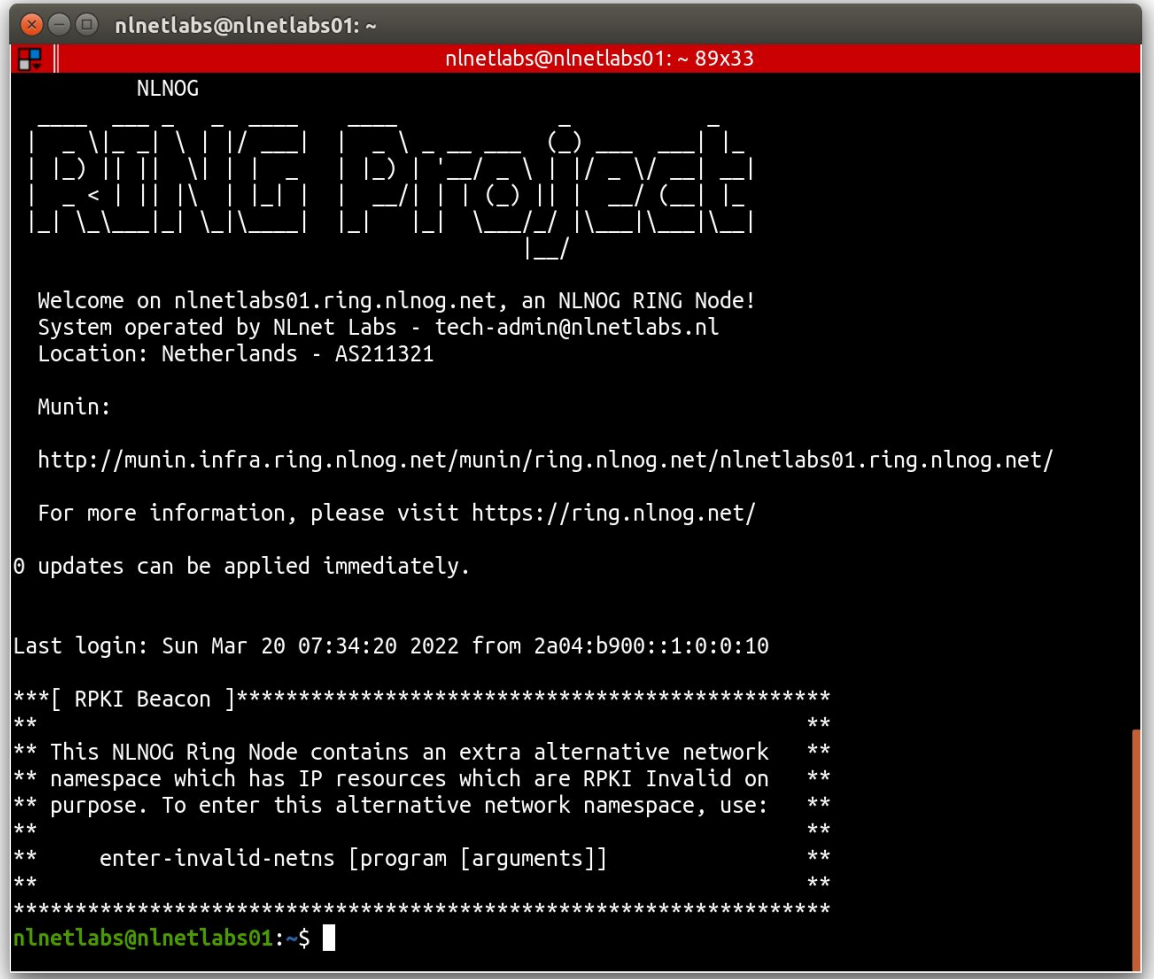
@ RIPE Atlas



DIY MSMs

@ RIPE Atlas

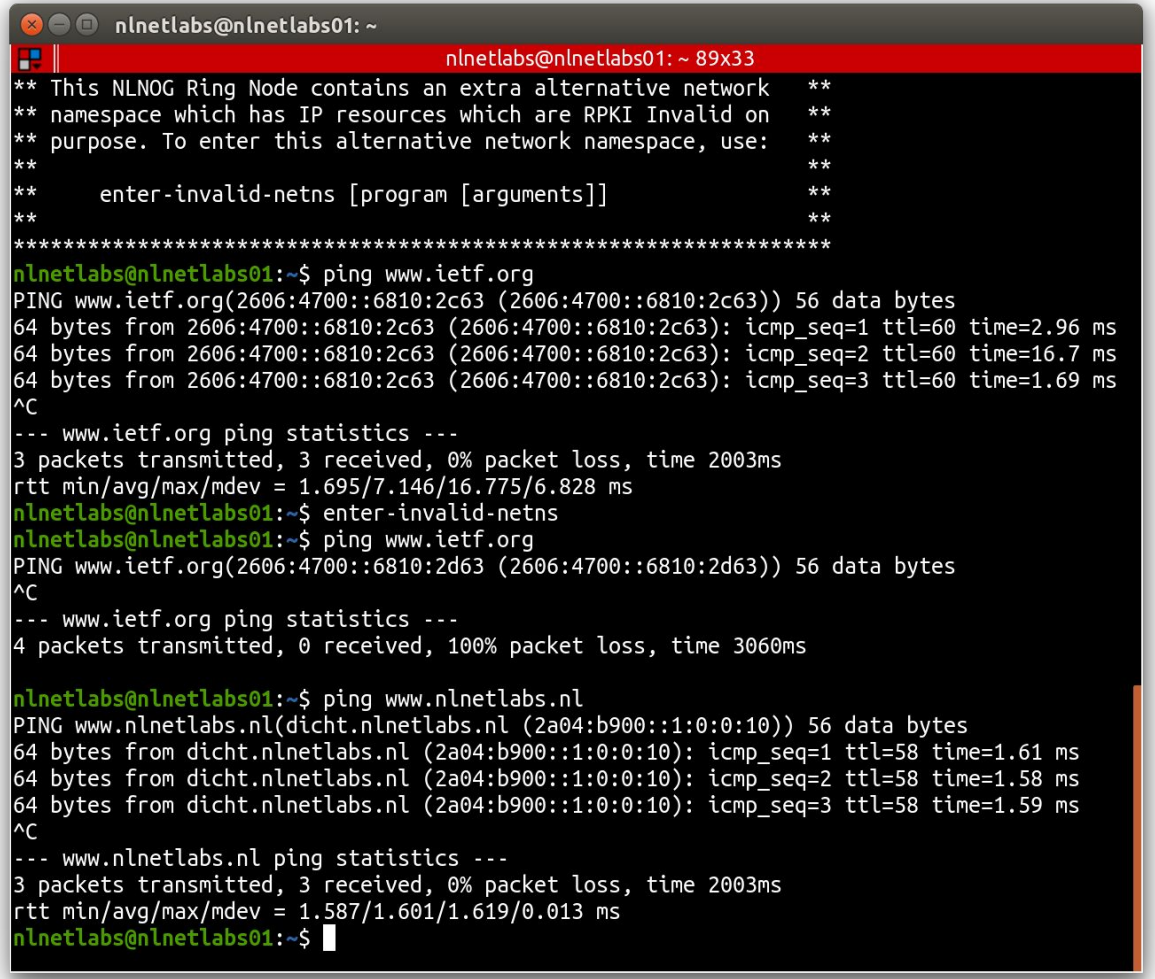
@ NLNOG Ring



DIY MSMs

@ RIPE Atlas

@ NLNOG Ring



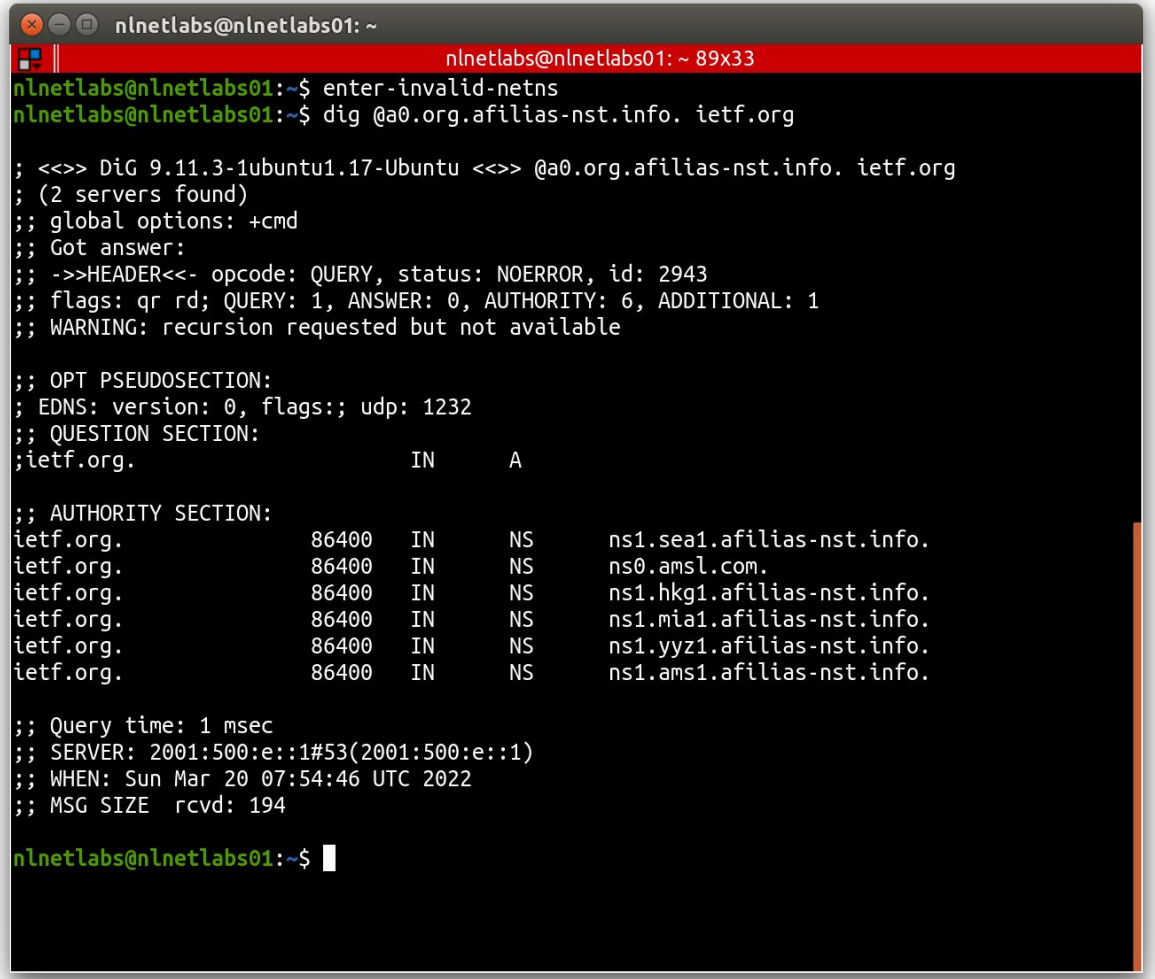
DIY MSMs

@ RIPE Atlas

@ NLNOG Ring

Meet diensten

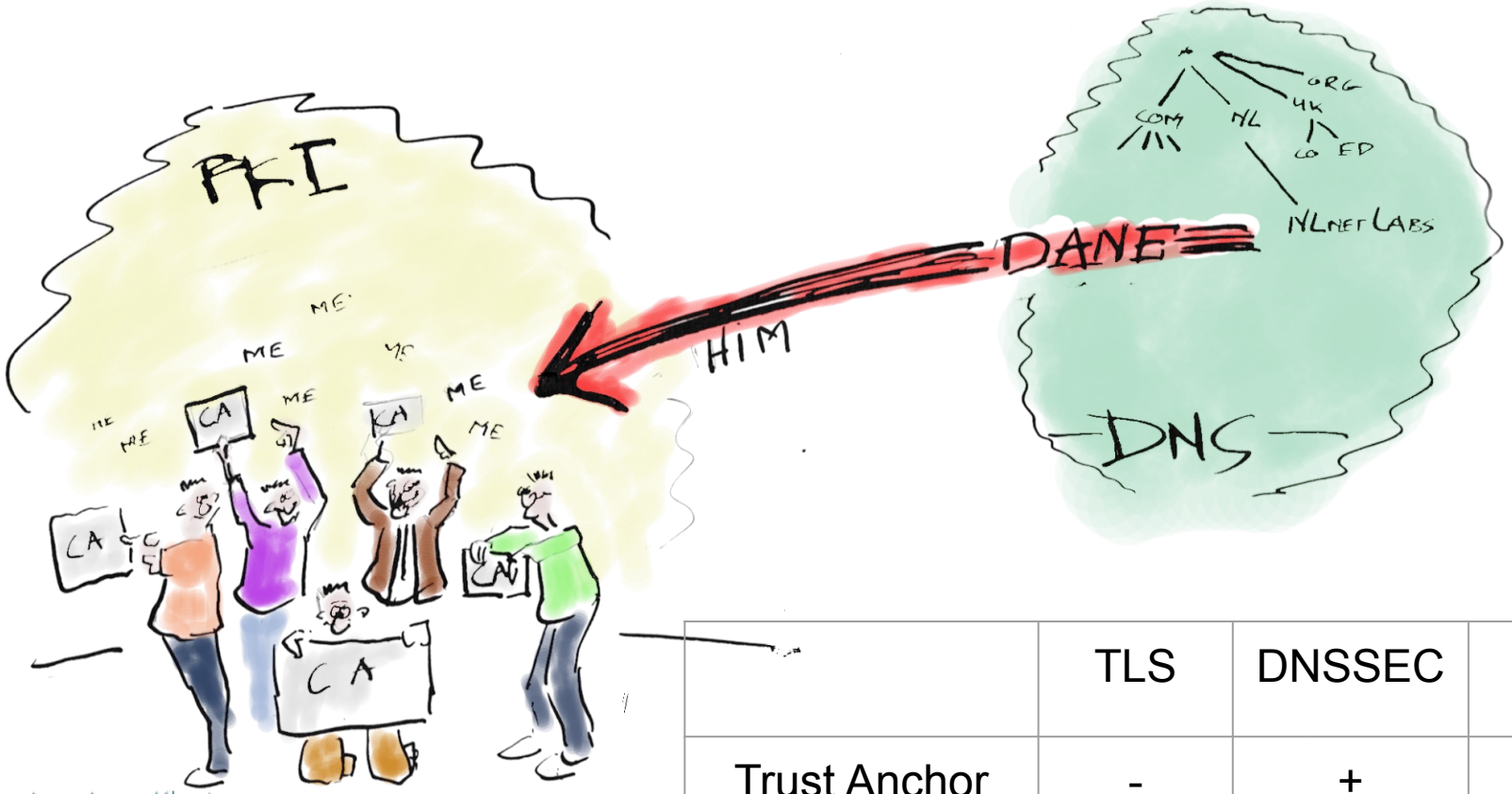
Moeten deze valideren?



TLS, DNSSEC en RPKI - evaluatie

	TLS	DNSSEC	RPKI
Trust Anchor	-	+	+-

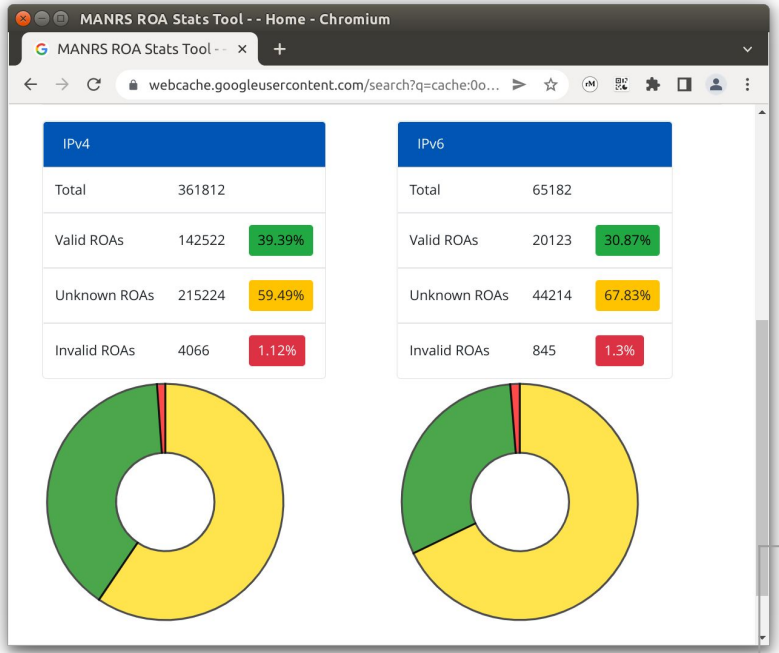
TLS, DNSSEC en RPKI - evaluatie

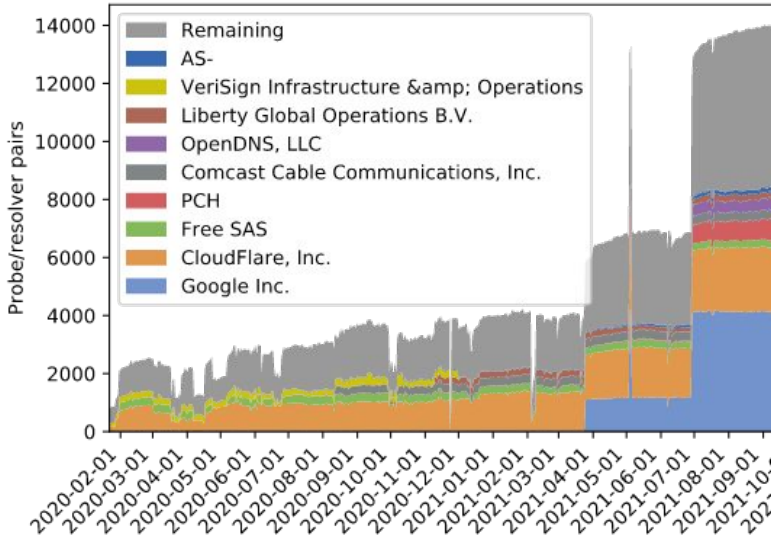


spotprent van Kloot

	TLS	DNSSEC	RPKI
Trust Anchor	-	+	+-

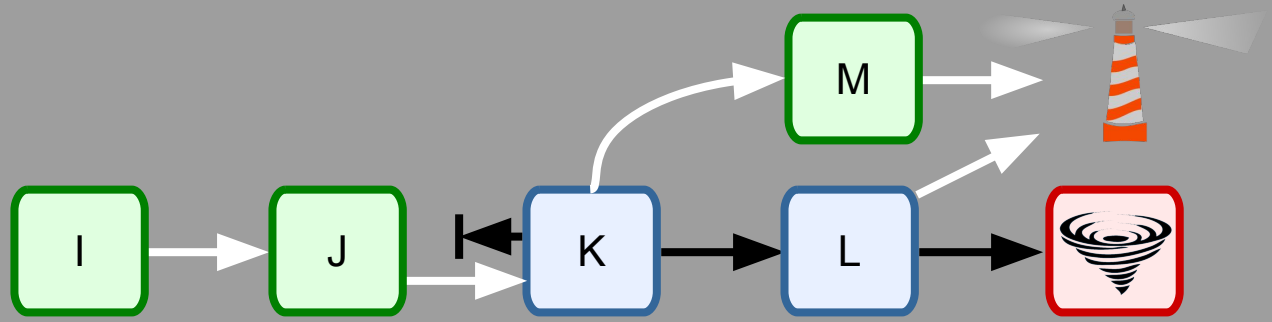
TLS, DNSSEC en RPKI - evaluatie





	TLS	DNSSEC	RPKI
Trust Anchor	-	+	+-
Verspreiding	++	--	+

TLS, DNSSEC en RPKI - evaluatie



	TLS	DNSSEC	RPKI
Trust Anchor	-	+	+-
Verspreiding	++	--	+
Eind naar Eind Secure	+	++	-

Het opzetten van een Resource Public Key Infrastructure (RPKI) baken

- Enkele bevindingen
  - Route Origin Validation is niet ja of nee
  - Voor een genuanceerde evaluatie
    - /24 een ongeldige – Eerste hops bescherming
    - /24 more specific hijack – Alle hops valideren
    - /24 hijack – Meer realistische hijack?
- Maakt RPKI een deel uit van jullie security policies?
- Suggesties voor toepassingen (tools) van het baken?
- Andere vragen?