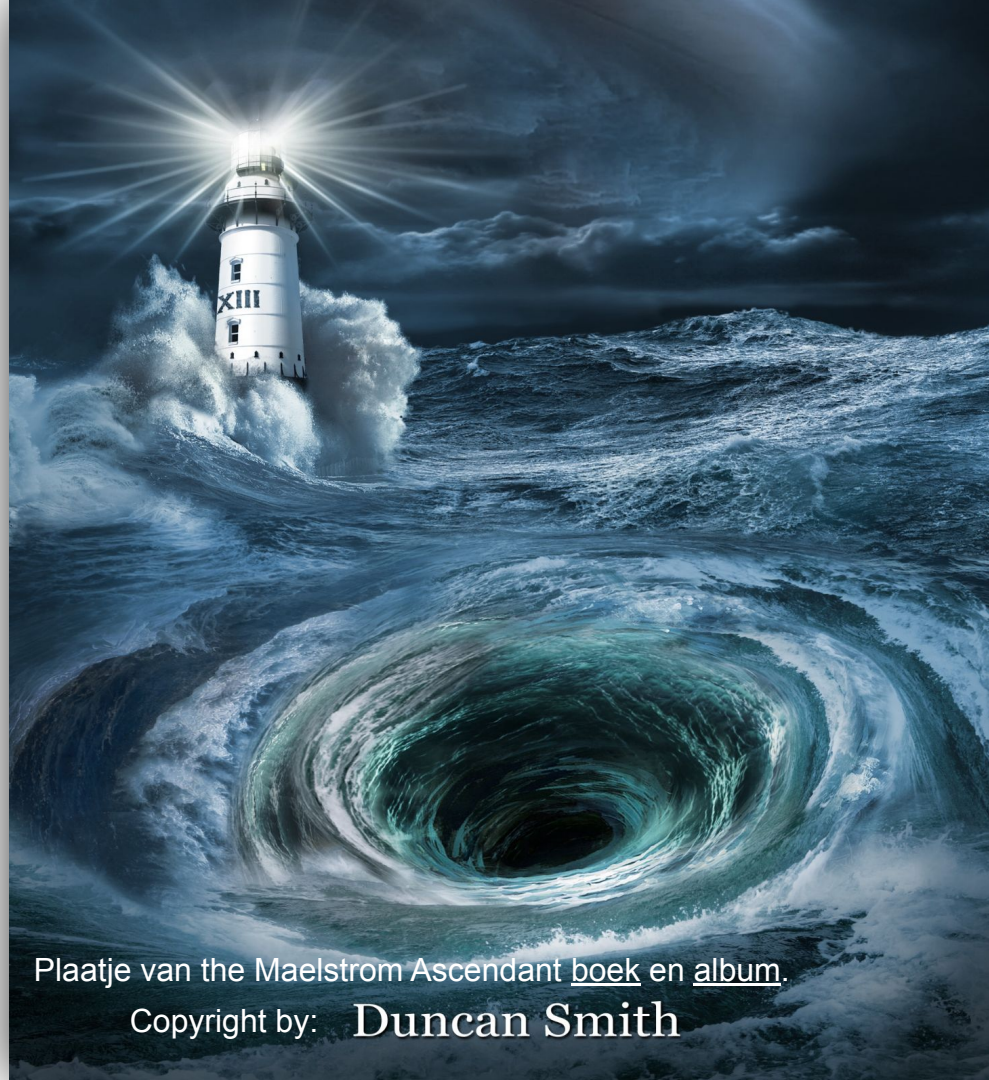


Het opzetten van een Resource Public Key Infrastructure (RPKI) baken

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

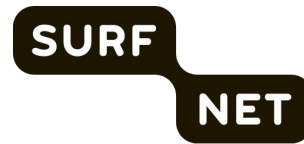
- Ik werk voor NLnet Labs en werk daar aan DNS software



- 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





- 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.*



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



- Idns
- Net::DNS
- Net::DNS::SEC

- Doel:



“

NLnet Labs writes code,
NLnet writes checks

– Michiel Leenaars

UTINATOR
Krill

- Idns
- Net::DNS
- Net::DNS::SEC

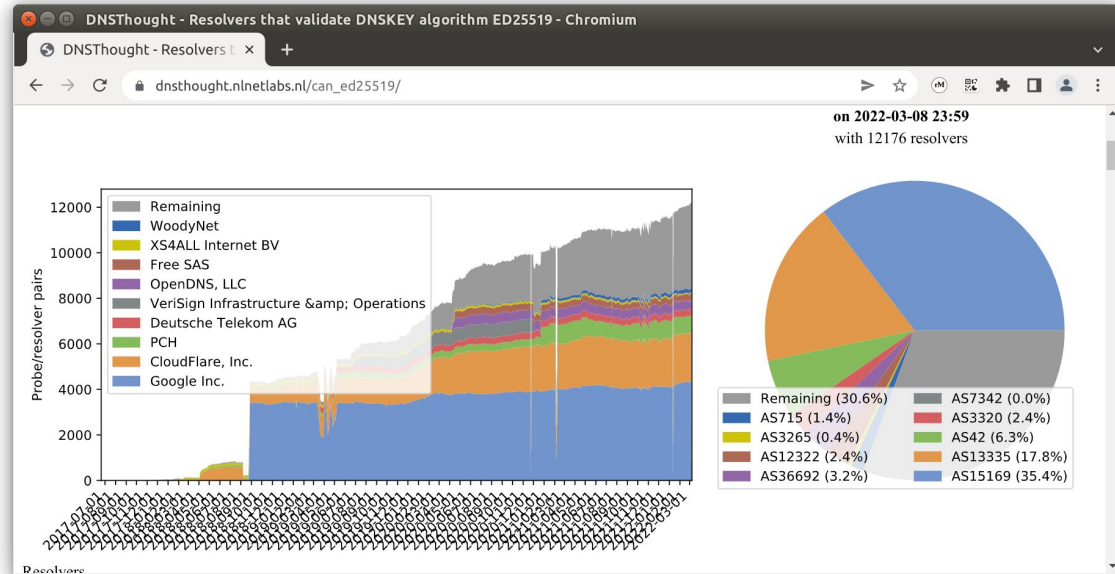


- Doel:
 - *Ontwikkelen van **Open Source software** en **Open Standaarden** ten behoeve van het Internet, en voorts al hetgeen met één en ander rechtstreeks of zijdelings verband houdt of daartoe bevorderlijk kan zijn, alles in de ruimste zin.*

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

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

What Happened? The Am x

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

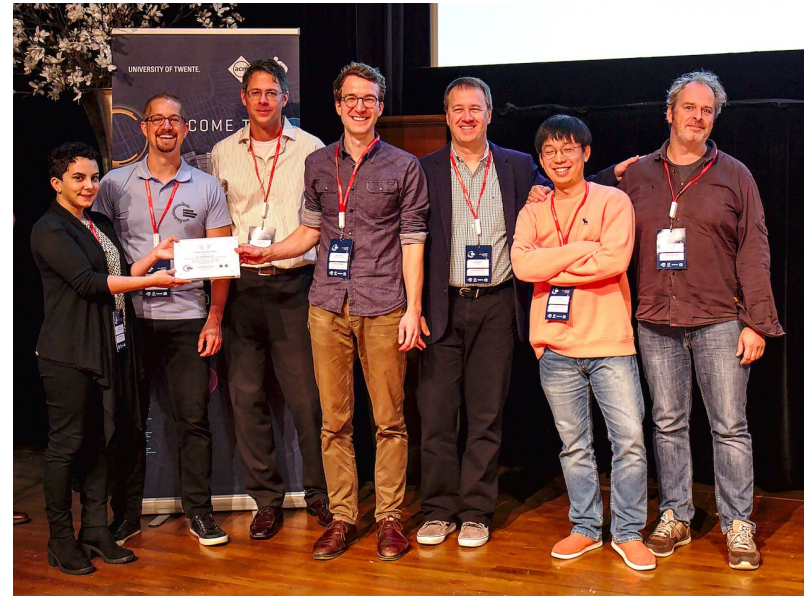
Yesterday, we published a blog post sharing the news and some initial details about [Amazon's DNS route hijack event to steal Ethereum cryptocurrency from myetherwallet.com](#). In this post, we'll explore more details about the incident from the BGP hijacker's perspective.

Software

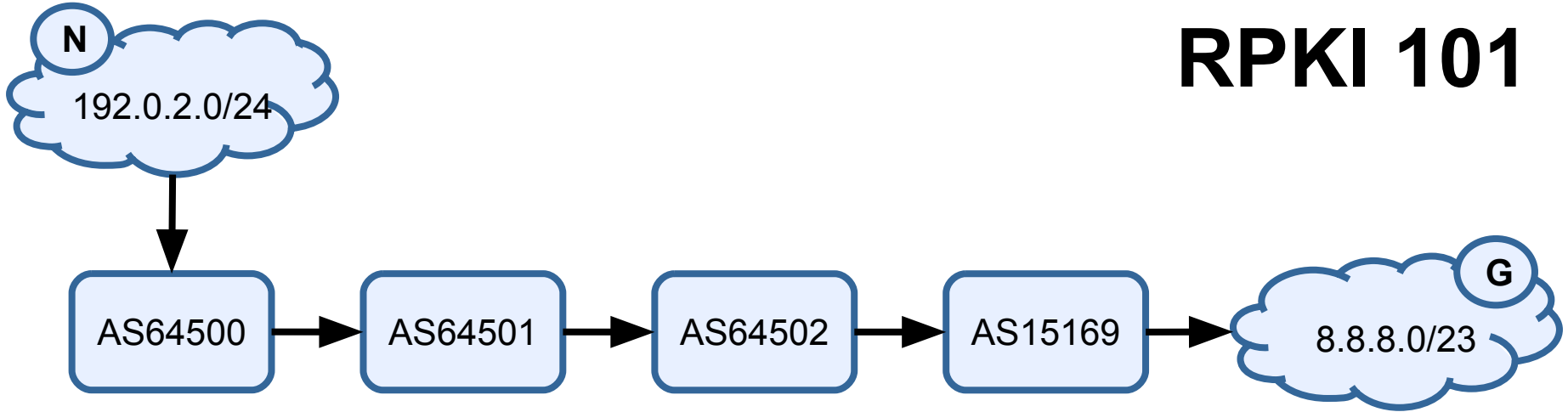


Ontstaan

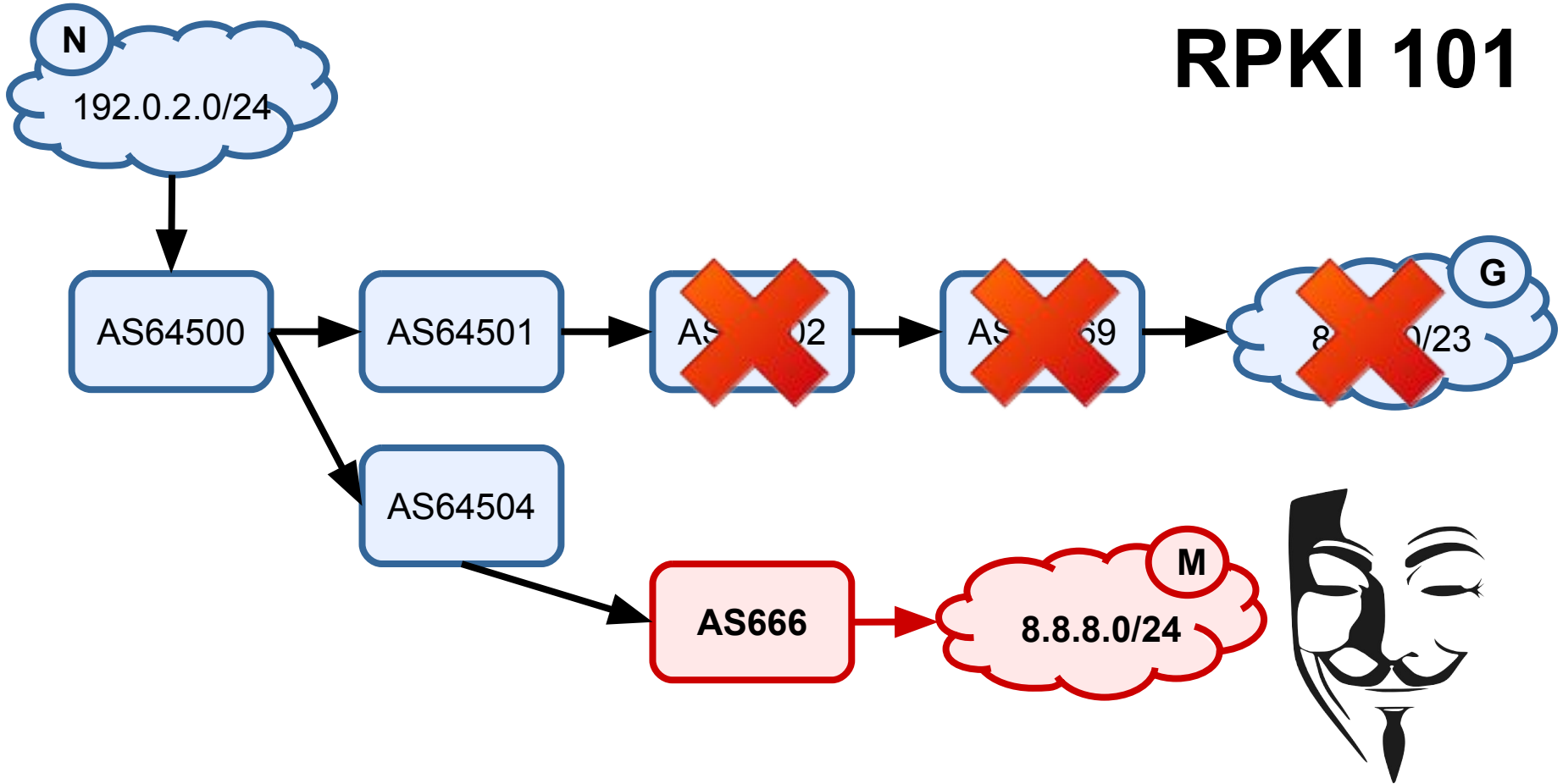
- Ik werk voor NLnet Labs en werk daar aan DNS software
- Ik doe ook metingen van DNS
- Job Snijders bood aan zijn RPKI baken te gebruiken bij IMC2019 in Amsterdam 🙏💖
- Begonnen met het meten van toename sinds januari 2022
- Job's baken EOL in okt. 2020



RPKI 101



RPKI 101



RPKI 101

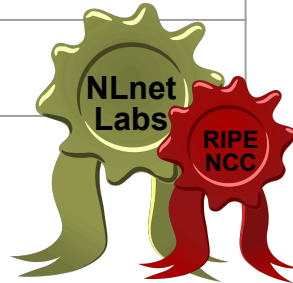
“an infrastructure to support improved security of Internet routing”

RFC6480

Tekenen (Signing)

- Route Origin Authorization

ASN	8587
Prefix	185.49.140.0/23
Max length	23

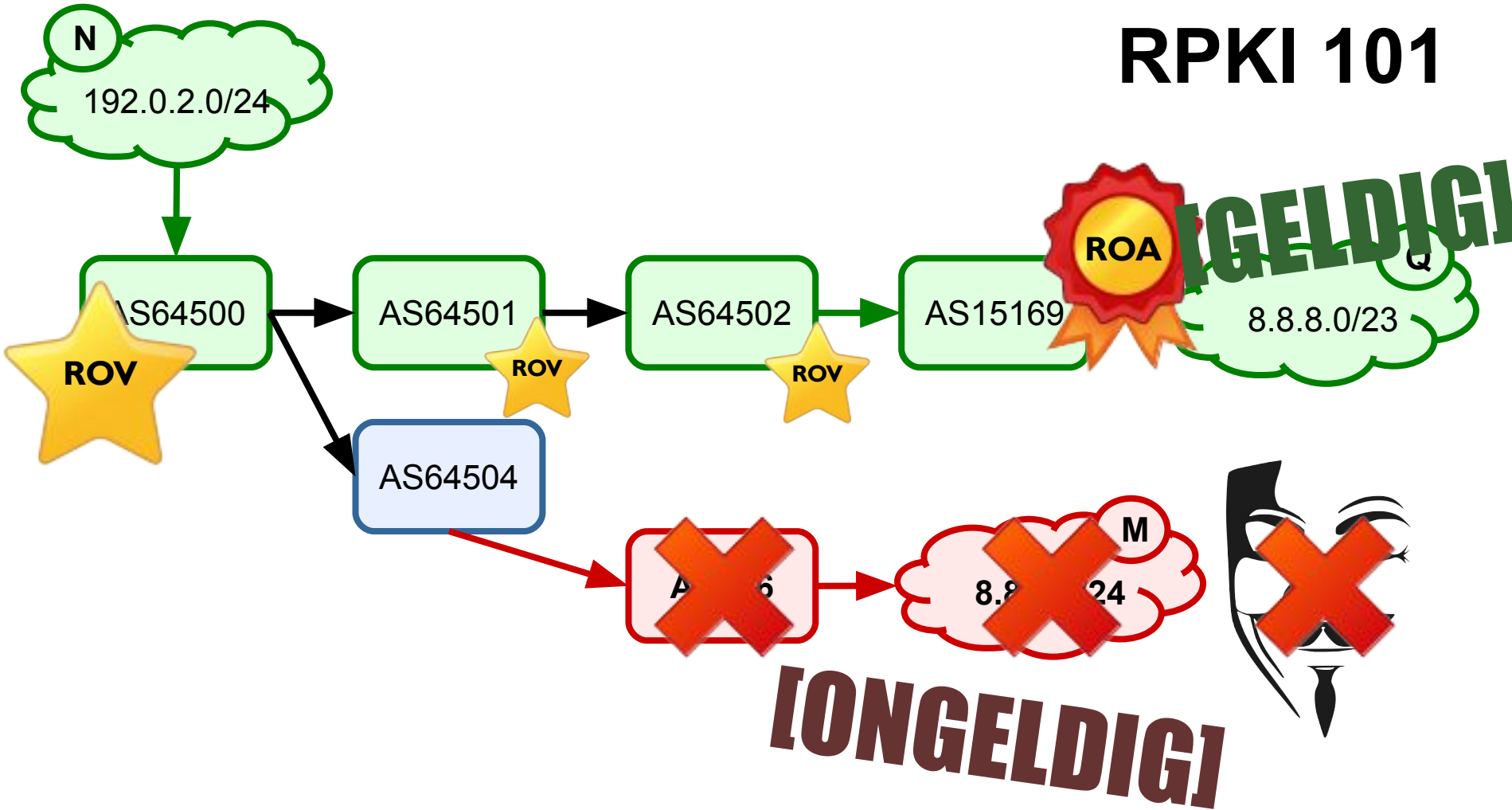


Validatie

- Route Origin Validation

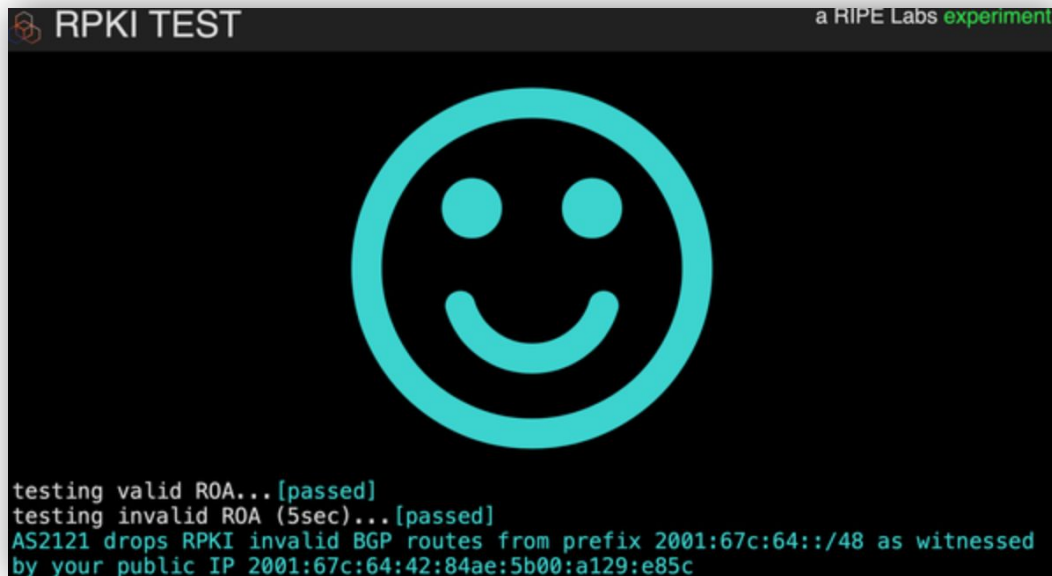
Voeg allen prefixes toe met een valide ROA

RPKI 101



Ontstaan

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



```
RPKI TEST a RIPE Labs experiment
testing valid ROA... [passed]
testing invalid ROA (5sec)... [passed]
AS2121 drops RPKI invalid BGP routes from prefix 2001:67c:64::/48 as witnessed
by your public IP 2001:67c:64:42:84ae:5b00:a129:e85c
```

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

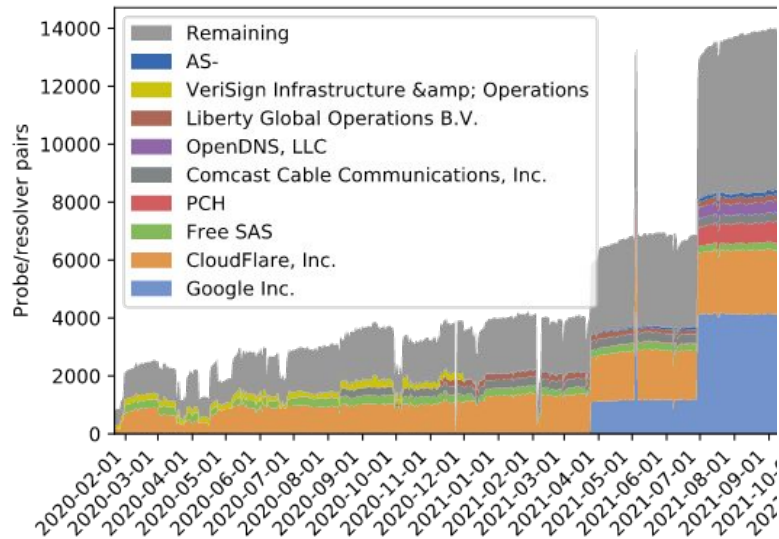
security, it is not broadly adopted [7, 8]. For this reason, this paper will focus on RPKI.

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].

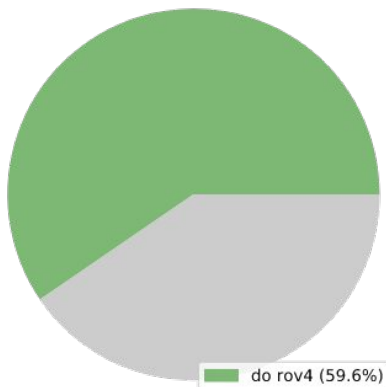
Non-RPKI filtered ASes could also benefit from RPKI when enough ASes have implemented RPKI filtering, e.g., when an AS lacks RPKI filtering, but one of its upstream ASes does not, the invalid prefix might still be filtered by one of its upstream ASes. However, there are still situations that one may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

Ontstaan

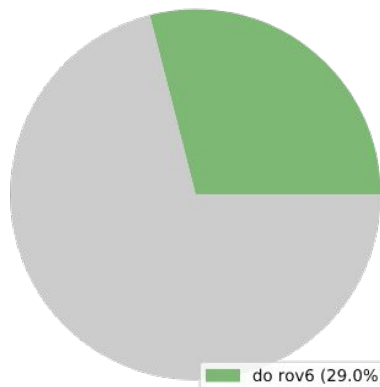
- Job's RPKI baken (pete.meervall.net) in gebruik door
 - RPKI NCC Web test
 - DNS-OARC's Check my DNS



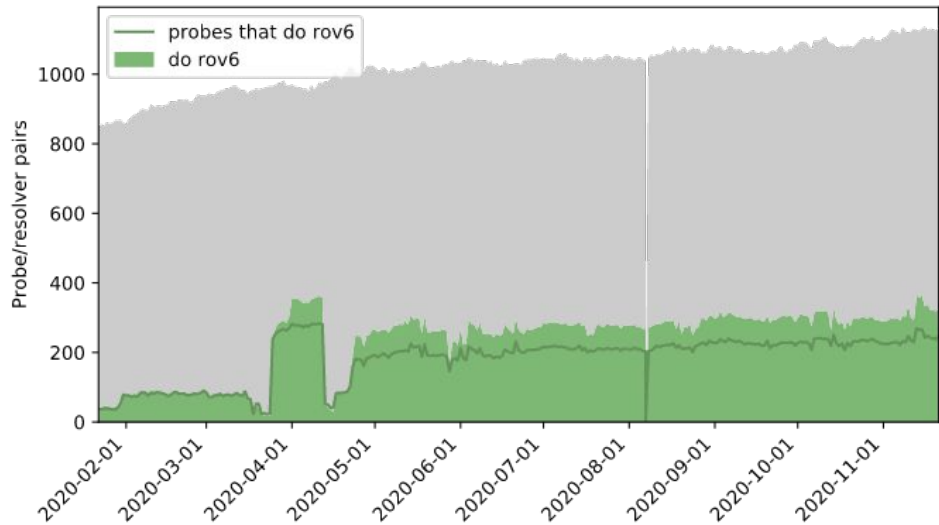
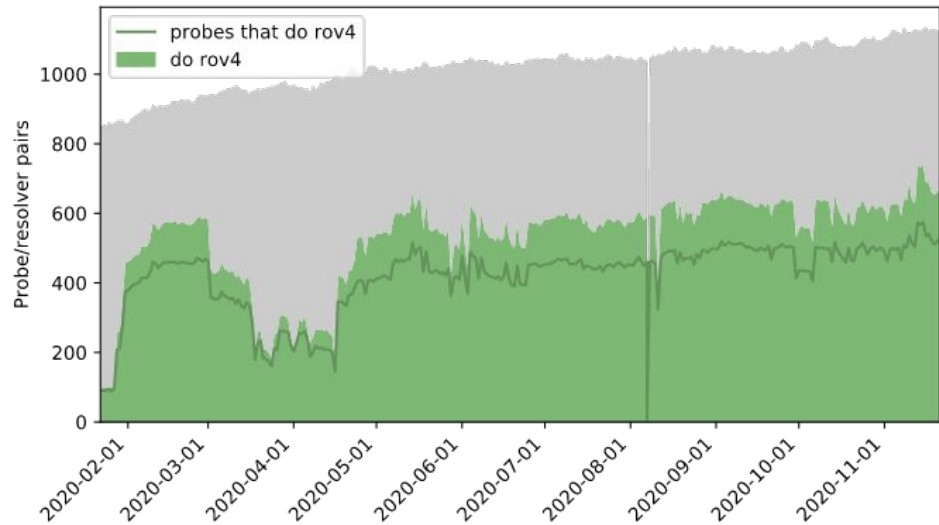
RoV van Cloudflare resolvers (AS13335)



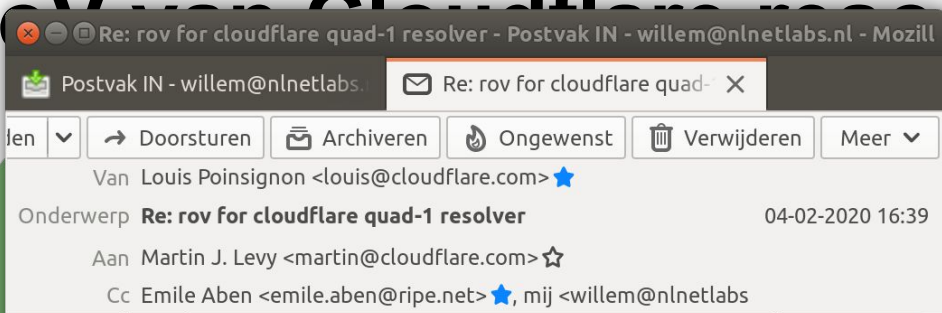
IPv4



IPv6



Router Cloudflare resolvers (AS13335)

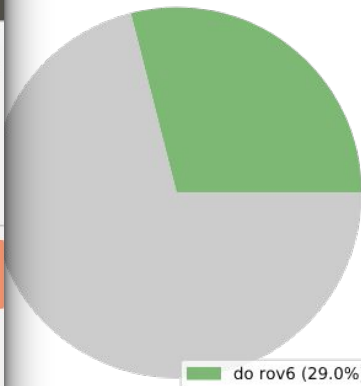


Once this is done, we should have all our routers dropping invalids.

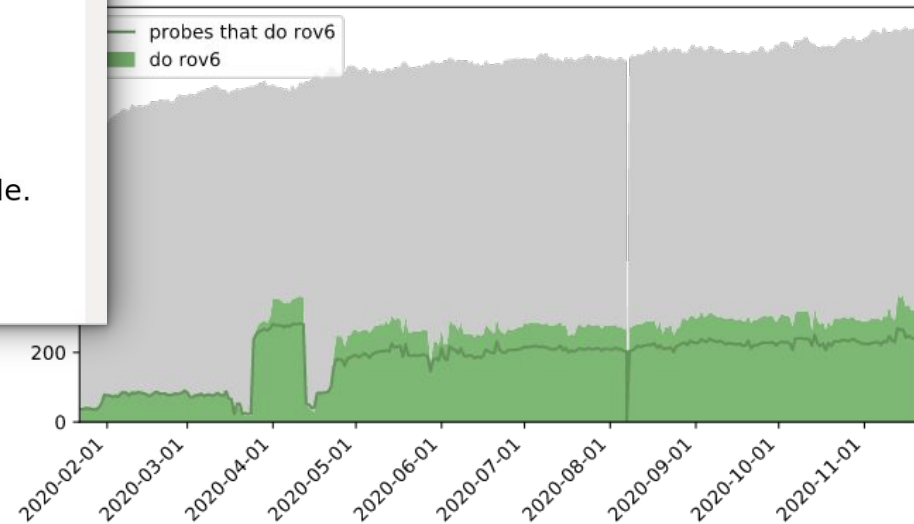
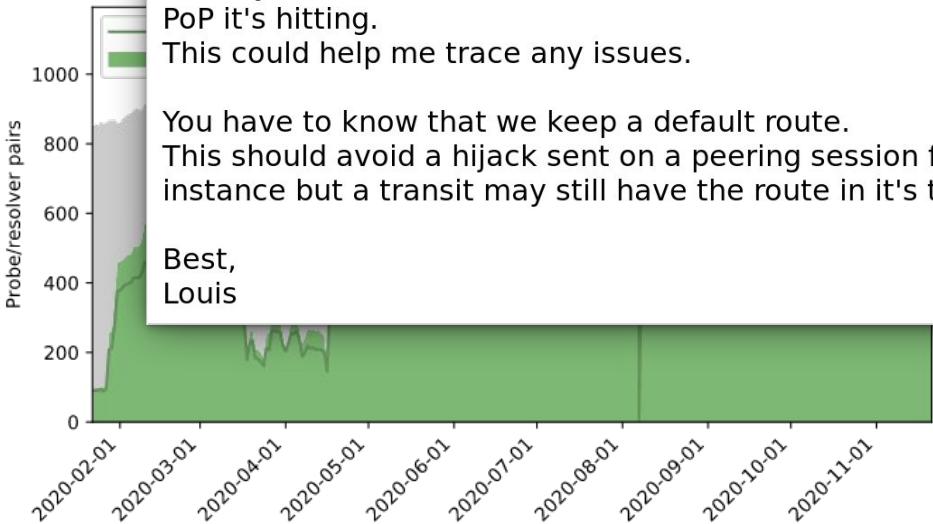
I'm assuming you're running DNS tests through Atlas?
Could you run a TXT CH bind.hostname, it should return the PoP it's hitting.
This could help me trace any issues.

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.

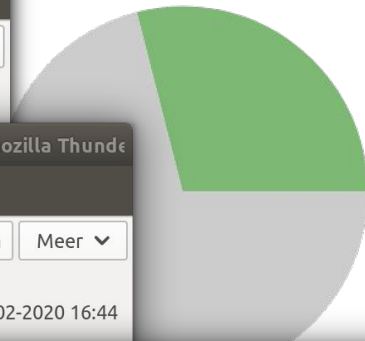
Best,
Louis



IPv6



Re: rovs for cloudflare quad-1 resolvers (AS13335)



IPv6

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

Postvak IN - willem@nlnetlabs.nl

Van Louis Poinsignon <louis@cloudflare.com>

Onderwerp: Re: rovs for cloudflare quad-1 resolver

04-02-2020 16:39

antwoorden

Doorsturen

Archiveren

Ongewenst

Verwijderen

Meer

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

Postvak IN - willem@nlnetlabs.nl

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

Onderwerp: Re: rovs for cloudflare quad-1 resolver

04-02-2020 16:44

Aan Louis Poinsignon <louis@cloudflare.com>

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

Once the resolvers are invalidated, I'm assuming you could yep. PoP it's this could be. You have this should be an instance. Best, Louis

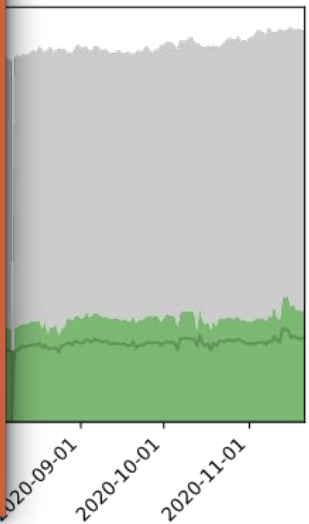
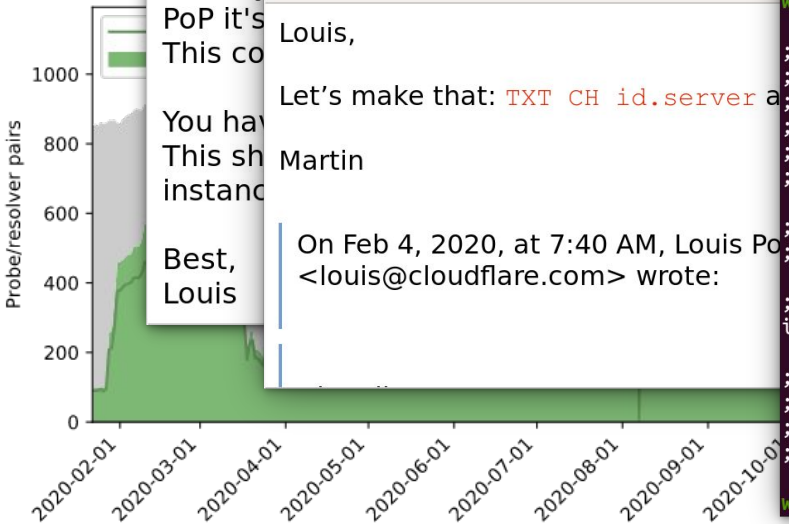
Louis,

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

Martin

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

```
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:~$
```



RoV van Cloudflare resolvers (AS13335) IPv4 - November 2020

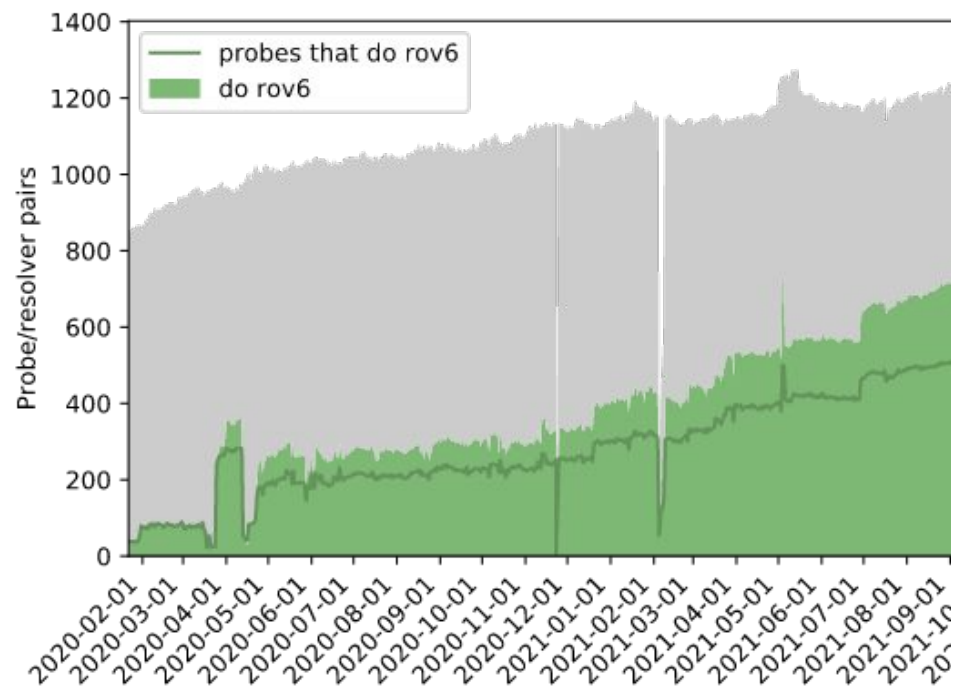
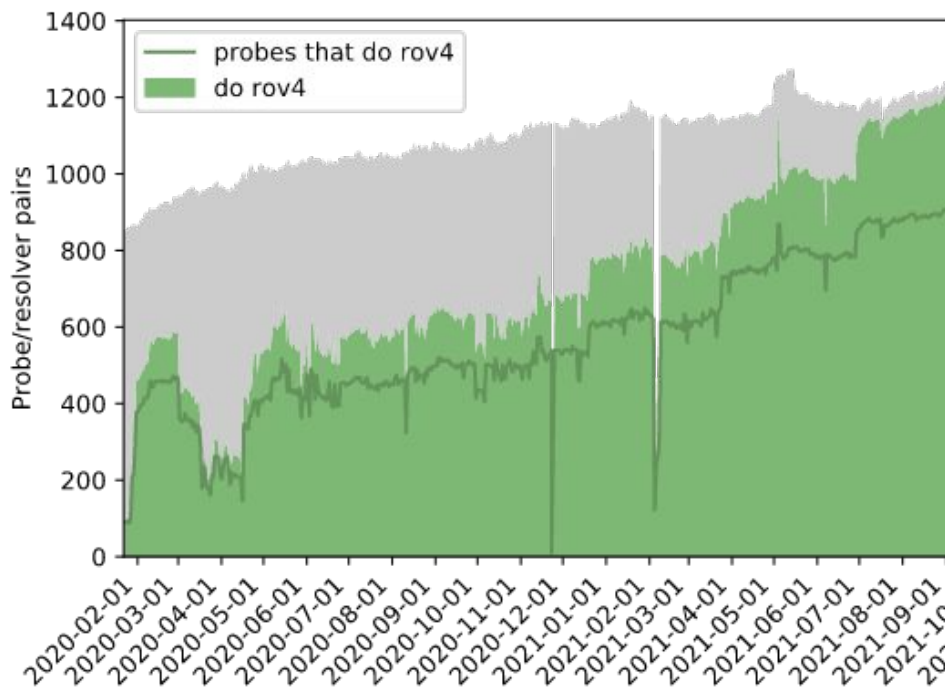


RoV van Cloudflare resolvers (AS13335) IPv6 - November 2020



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.
```

```
$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	209.24.1.0/24
max len	24
ASN	15562

[GELDIG]

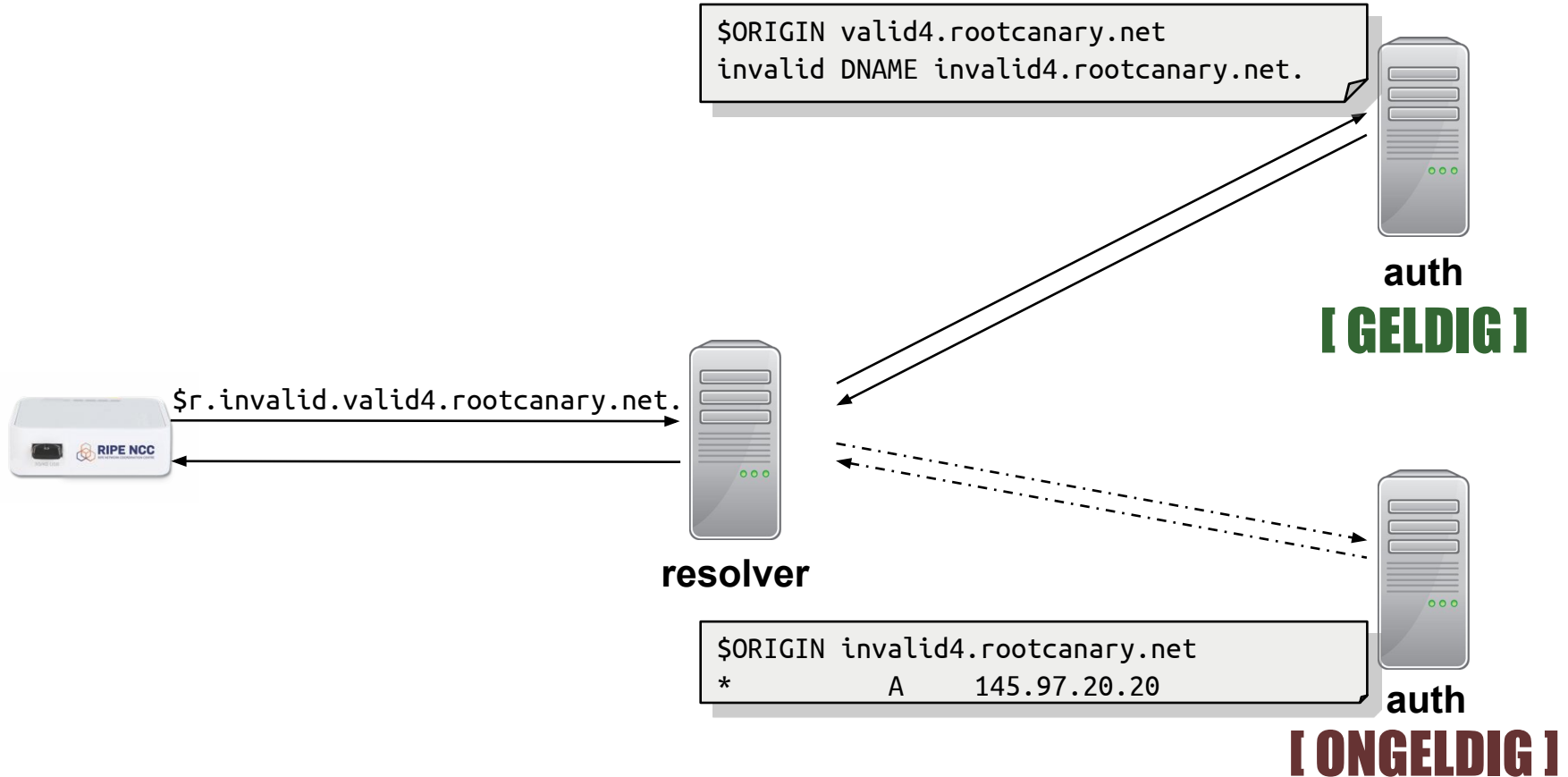


prefix	194.32.71.0/24
max len	24
ASN	0

[ONGELDIG]



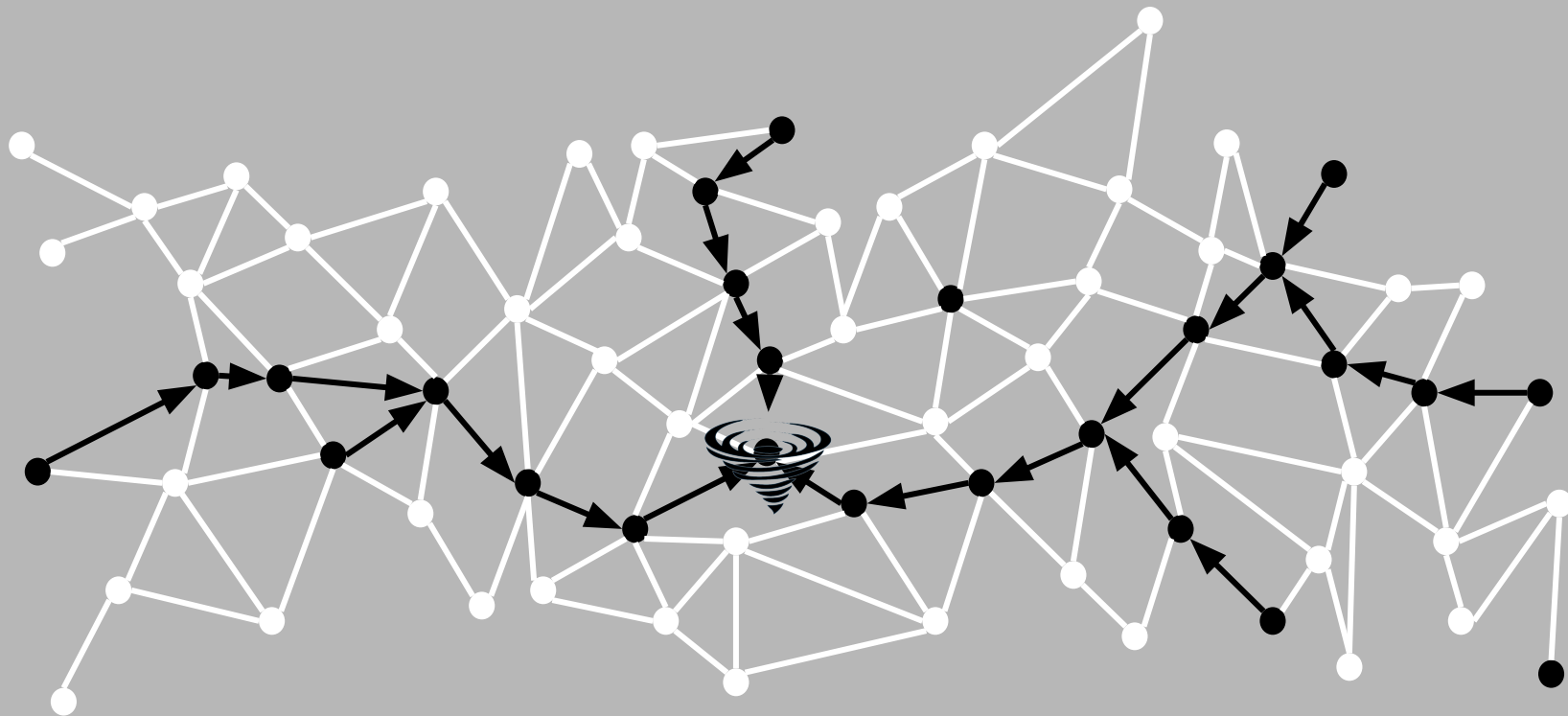
Herevaluatie baken - voorheen



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



Krill - RPKI - Chromium

Krill - RPKI

prod-ca.krill.cloud/index.html#/cas/nlnetlabs

Nederlands

Krill

Certificaatautoriteit **nlnetlabs**

ROAs Bovenliggende CAs Databank (repository)

185.49.142.0 Download CSV

ASN	Prefix	Status	
> 0	185.49.142.0/24-24	OVERBODIG	
> 16509	185.49.142.0/23-23	ZICHTBAAR 1 1	
211321	185.49.142.0/24	ONGELDIG ASN	

25/page < 1 >

Voeg ROA toe Analyseer mijn ROAs

neouts)

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

- Geldig /23 (IF more specific)
- ✓ Een meer
- ✓ Geen dete
- x We weten
- x Zelfs als
- kun je no



Afbeelding van de Maelstrom Ascendant [boek](#) en [album](#).

Copyright by: **Duncan Smith**

etup

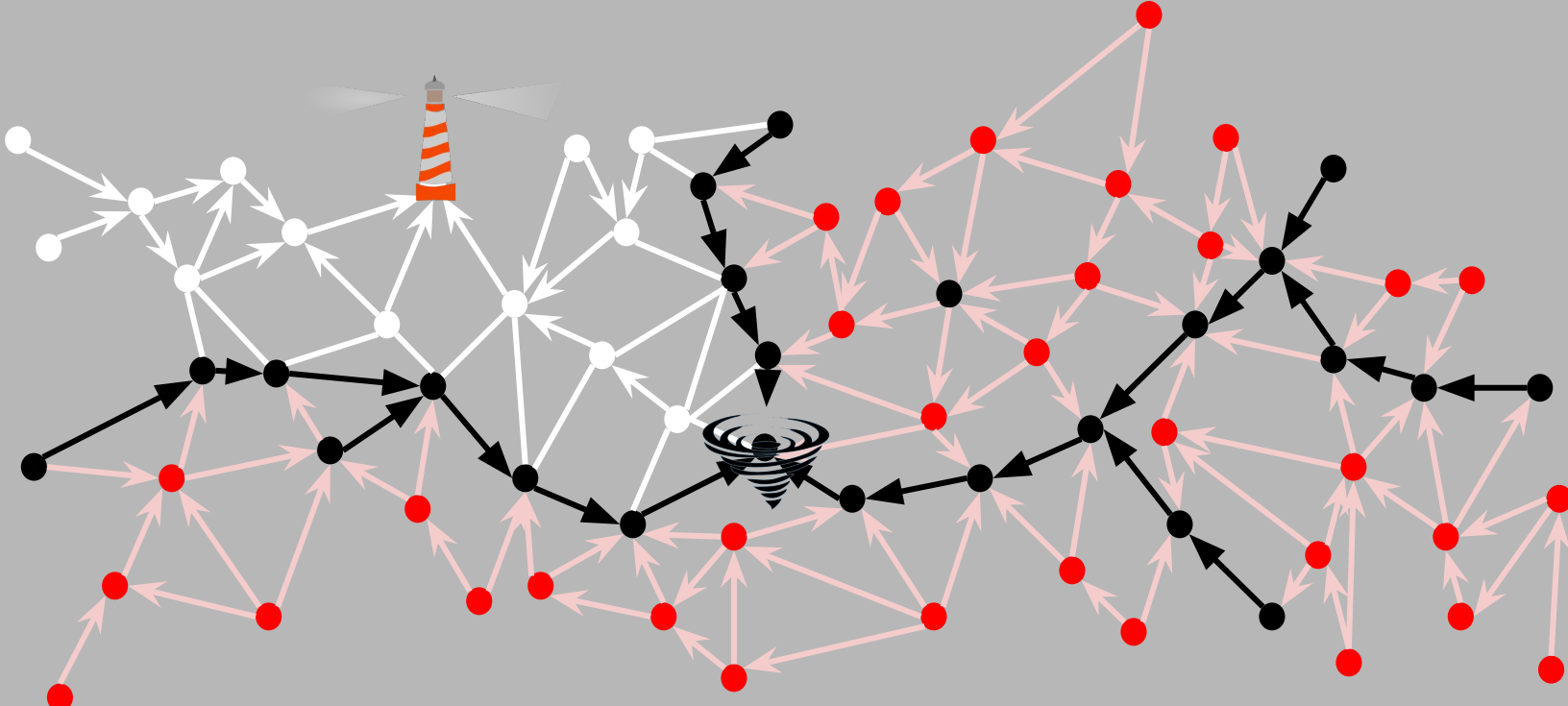
en /48

eid (geen timeouts)

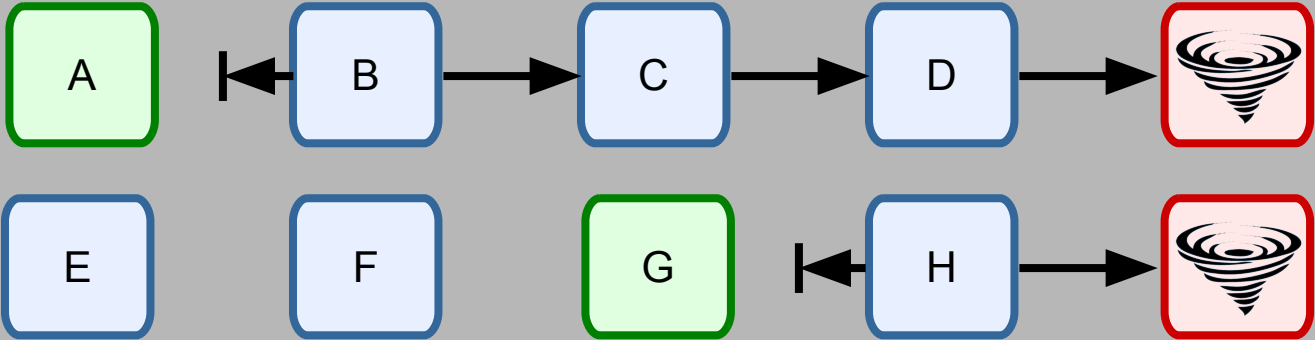
rt

d) uitkomen!

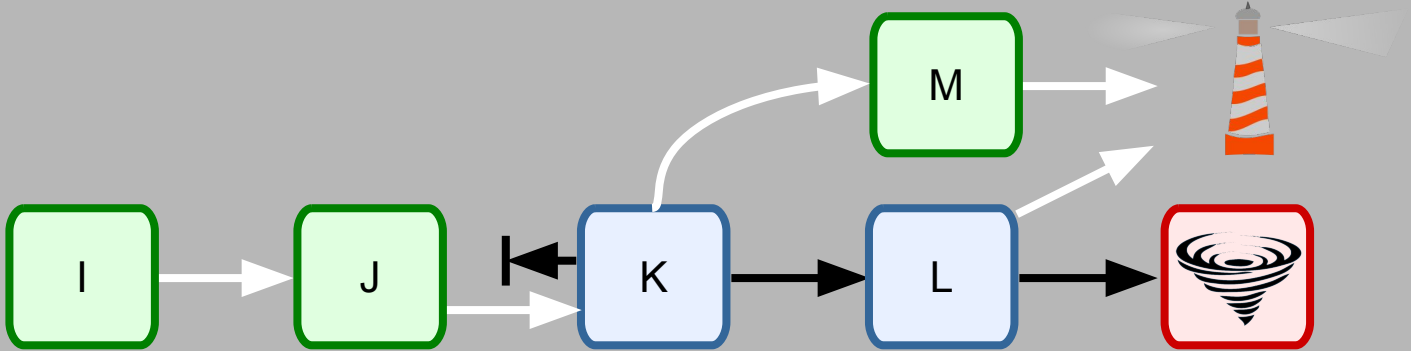
Herevaluatie baken - nieuwe setup



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!!!



[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 winst oogmerk, 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.

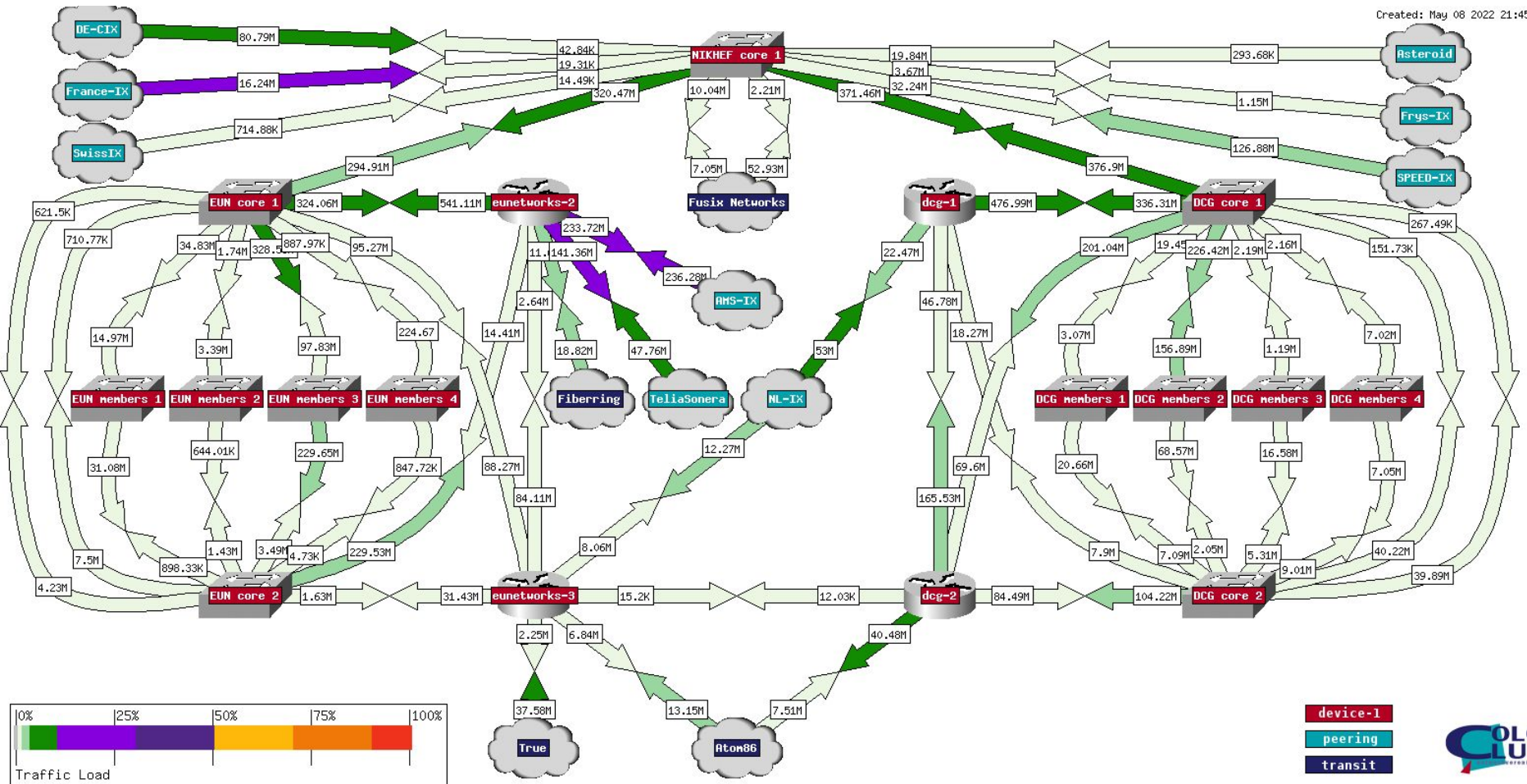
CLUEMETER

April 2022

Racks : 8

Machines : 127

Leden : 191



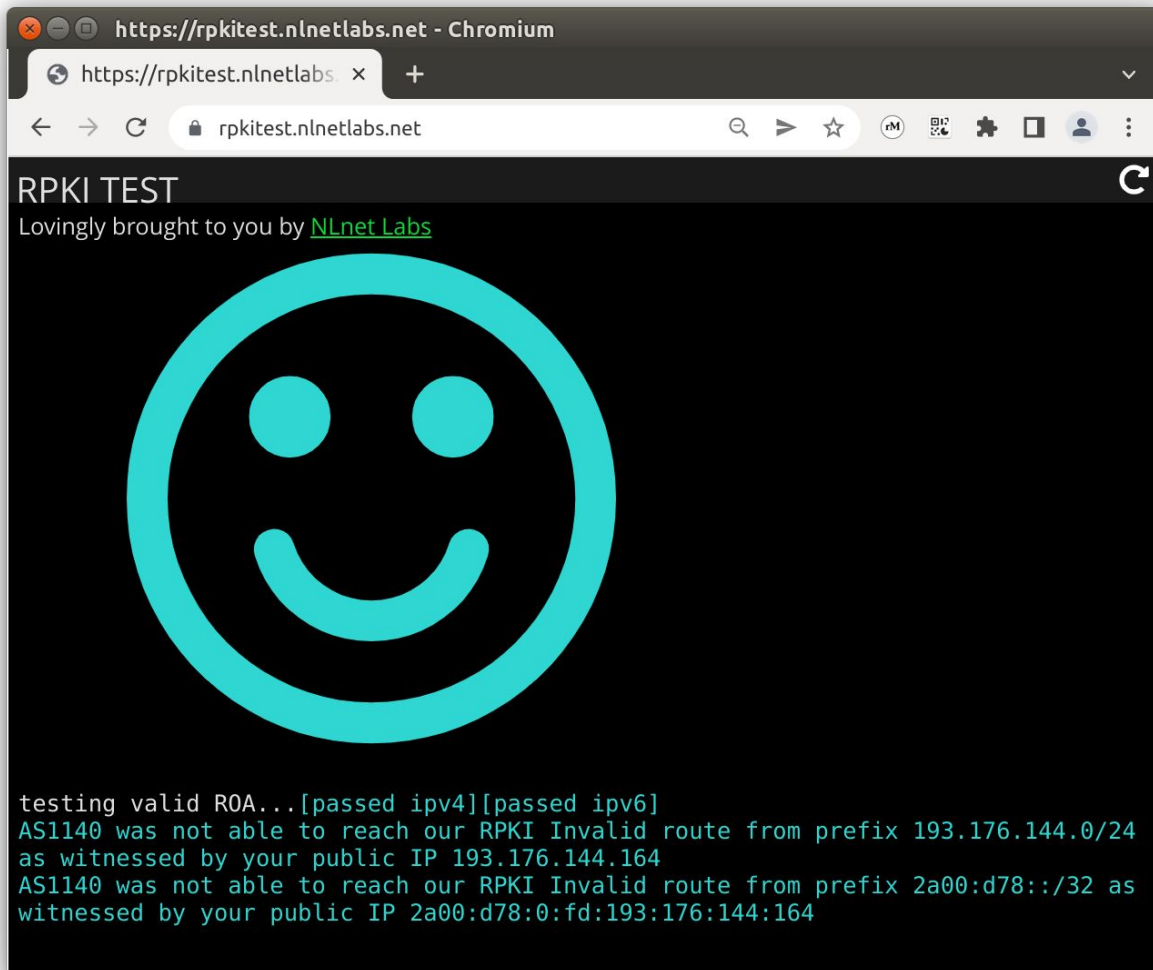
Tools

- Resolver test:
onmiddellijk
resultaat! 👍

```
willem@makaak: ~  
willem@makaak: ~ 80x24  
willem@makaak:~$ dig @1.1.1.1 rpkitest4.nl netlabs.nl TXT  
;  
;<<> DiG 9.16.15-Ubuntu <<> @1.1.1.1 rpkitest4.nl netlabs.nl TXT  
;(1 server found)  
;; global options: +cmd  
;; Got answer:  
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 36209  
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1  
;  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags:;; udp: 1232  
;; QUESTION SECTION:  
;rpkitest4.nl netlabs.nl.  
IN TXT  
;  
;; ANSWER SECTION:  
rpkitest4.nl netlabs.nl. 1 IN TXT "HOORAY - Your resolver is protected by Route Origin Validation :)"  
;  
;; Query time: 32 msec  
;; SERVER: 1.1.1.1#53(1.1.1.1)  
;; WHEN: do mrt 17 15:41:43 CET 2022  
;; MSG SIZE rcvd: 130  
willem@makaak:~$
```

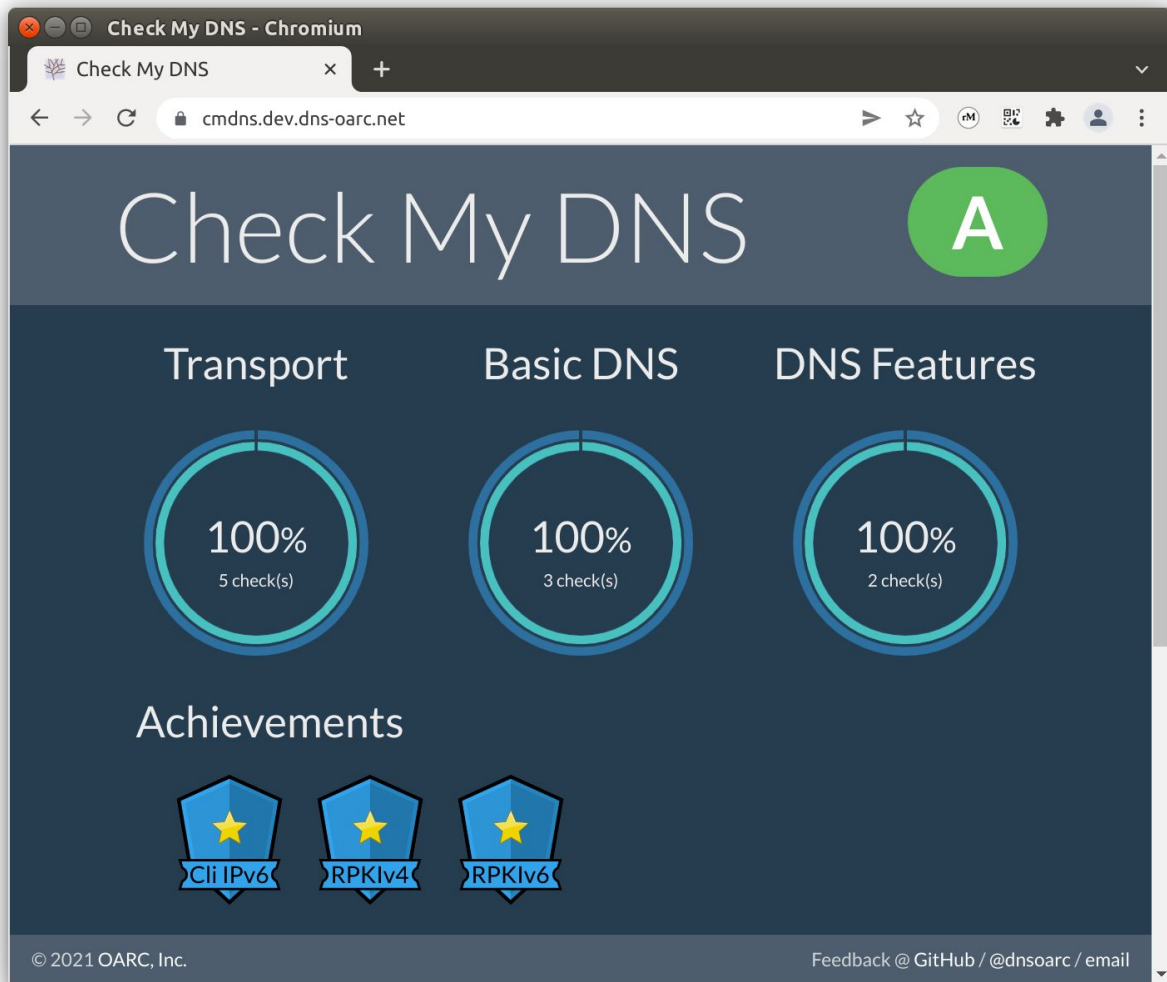
Tools

- 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

The screenshot shows the RIPE Atlas interface for a specific probe. The browser address bar indicates the URL is `atlas.ripe.net/probes/1003688/#tab-network`. The main heading is "Probe on RPKI Invalid resources". Below this, there are tabs for "General", "Network", "Built-ins", "UDMs", and "Status (beta)". The "Network" tab is active, showing configuration for both IPv4 and IPv6. The IPv4 section includes fields for Internet Address, ASN, Local Address, Gateway, Netmask, and DNS_Resolvers. The IPv6 section includes fields for Addresses, ASN, Gateway(s), and DNS_Resolvers. A "Probe Address Discovery" table is also present, comparing IPv4 and IPv6 connection addresses, IP Echo Service, and the local IP. On the right side, there is a sidebar with the probe ID "#1003688", a "1 week" timer, and fields for Firmware, Architecture, and MAC Address. A green "Update Location" button is visible below the sidebar. At the bottom right, there is a map showing the probe's location in Hembrug, with a green pin and a large "RIPE" watermark.

Probe on RPKI Invalid resources

General Network Built-ins UDMs Status (beta)

IPv4

Current Configuration

Internet Address	185.49.142.11
ASN	211321 (NLNETLABS - Stichting NLnet Labs)
Local Address	185.49.142.11
Gateway	185.49.142.1
Netmask	255.255.255.0
DNS_Resolvers	185.49.142.1

IPv6

Current Configuration

Addresses	2a04:b904::11/64 2a04:b907::11/64
ASN	211321 (NLNETLABS - Stichting NLnet Labs)
Gateway(s)	2a04:b907::1 2a04:b904::1
DNS_Resolvers	2a04:b907::1

Probe Address Discovery

	IPv4	IPv6
Connection Address	-	✓ 2a04:b904::11
IP Echo Service	-	-
The Local IP	✓ 185.49.142.11	2a04:b907::11

Update Location

DIY MSMs

@ RIPE Atlas

@ NLNOG Ring

```
nlnetlabs@nlnetlabs01: ~
nlnetlabs@nlnetlabs01: ~ 89x33
NLNOG
RING Project

Welcome on nlnetlabs01.ring.nlnog.net, an NLNOG RING Node!
System operated by NLnet Labs - tech-admin@nlnetlabs.nl
Location: Netherlands - AS211321

Munin:

http://munin.infra.ring.nlnog.net/munin/ring.nlnog.net/nlnetlabs01.ring.nlnog.net/

For more information, please visit https://ring.nlnog.net/

0 updates can be applied immediately.

Last login: Sun Mar 20 07:34:20 2022 from 2a04:b900::1:0:0:10

***[ RPKI Beacon ]*****
**
** This NLNOG Ring Node contains an extra alternative network **
** namespace which has IP resources which are RPKI Invalid on **
** purpose. To enter this alternative network namespace, use: **
**
**   enter-invalid-netns [program [arguments]] **
**
*****
nlnetlabs@nlnetlabs01:~$
```

DIY MSMs

@ RIPE Atlas

@ NLNOG Ring

```
nlnetlabs@nlnetlabs01: ~
nlnetlabs@nlnetlabs01: ~ 89x33
** This NLNOG Ring Node contains an extra alternative network namespace which has IP resources which are RPKI Invalid on purpose. To enter this alternative network namespace, use:
**
** enter-invalid-netns [program [arguments]]
**
*****
nlnetlabs@nlnetlabs01:~$ ping www.ietf.org
PING www.ietf.org(2606:4700::6810:2c63 (2606:4700::6810:2c63)) 56 data bytes
64 bytes from 2606:4700::6810:2c63 (2606:4700::6810:2c63): icmp_seq=1 ttl=60 time=2.96 ms
64 bytes from 2606:4700::6810:2c63 (2606:4700::6810:2c63): icmp_seq=2 ttl=60 time=16.7 ms
64 bytes from 2606:4700::6810:2c63 (2606:4700::6810:2c63): icmp_seq=3 ttl=60 time=1.69 ms
^C
--- www.ietf.org ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 1.695/7.146/16.775/6.828 ms
nlnetlabs@nlnetlabs01:~$ enter-invalid-netns
nlnetlabs@nlnetlabs01:~$ ping www.ietf.org
PING www.ietf.org(2606:4700::6810:2d63 (2606:4700::6810:2d63)) 56 data bytes
^C
--- www.ietf.org ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3060ms

nlnetlabs@nlnetlabs01:~$ ping www.nlnetlabs.nl
PING www.nlnetlabs.nl(dicht.nlnetlabs.nl (2a04:b900::1:0:0:10)) 56 data bytes
64 bytes from dicht.nlnetlabs.nl (2a04:b900::1:0:0:10): icmp_seq=1 ttl=58 time=1.61 ms
64 bytes from dicht.nlnetlabs.nl (2a04:b900::1:0:0:10): icmp_seq=2 ttl=58 time=1.58 ms
64 bytes from dicht.nlnetlabs.nl (2a04:b900::1:0:0:10): icmp_seq=3 ttl=58 time=1.59 ms
^C
--- www.nlnetlabs.nl ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 1.587/1.601/1.619/0.013 ms
nlnetlabs@nlnetlabs01:~$
```

DIY MSMs

@ RIPE Atlas

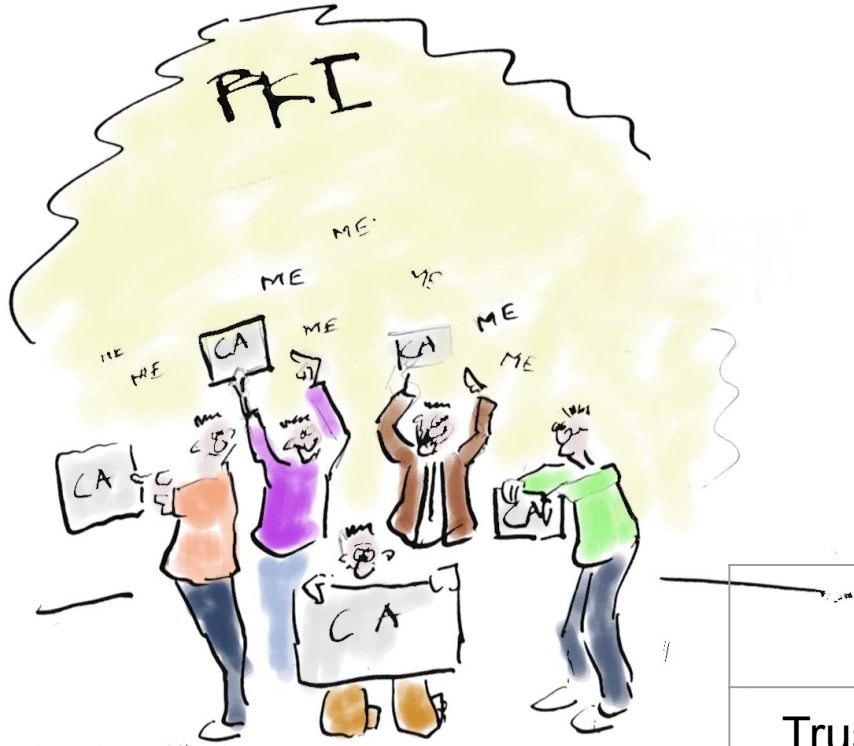
@ NLNOG Ring

Meet diensten

Moeten deze
valideren?

```
nlnetlabs@nlnetlabs01: ~  
nlnetlabs@nlnetlabs01:~$ enter-invalid-netns  
nlnetlabs@nlnetlabs01:~$ dig @a0.org.afilias-nst.info. ietf.org  
  
; <<>> DiG 9.11.3-1ubuntu1.17-Ubuntu <<>> @a0.org.afilias-nst.info. ietf.org  
; (2 servers found)  
;; global options: +cmd  
;; Got answer:  
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 2943  
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 6, ADDITIONAL: 1  
;; WARNING: recursion requested but not available  
  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags:; udp: 1232  
;; QUESTION SECTION:  
;ietf.org.                IN      A  
  
;; AUTHORITY SECTION:  
ietf.org.                86400  IN      NS      ns1.sea1.afilias-nst.info.  
ietf.org.                86400  IN      NS      ns0.amsl.com.  
ietf.org.                86400  IN      NS      ns1.hkg1.afilias-nst.info.  
ietf.org.                86400  IN      NS      ns1.mia1.afilias-nst.info.  
ietf.org.                86400  IN      NS      ns1.yyz1.afilias-nst.info.  
ietf.org.                86400  IN      NS      ns1.ams1.afilias-nst.info.  
  
;; Query time: 1 msec  
;; SERVER: 2001:500:e::1#53(2001:500:e::1)  
;; WHEN: Sun Mar 20 07:54:46 UTC 2022  
;; MSG SIZE rcvd: 194  
  
nlnetlabs@nlnetlabs01:~$
```

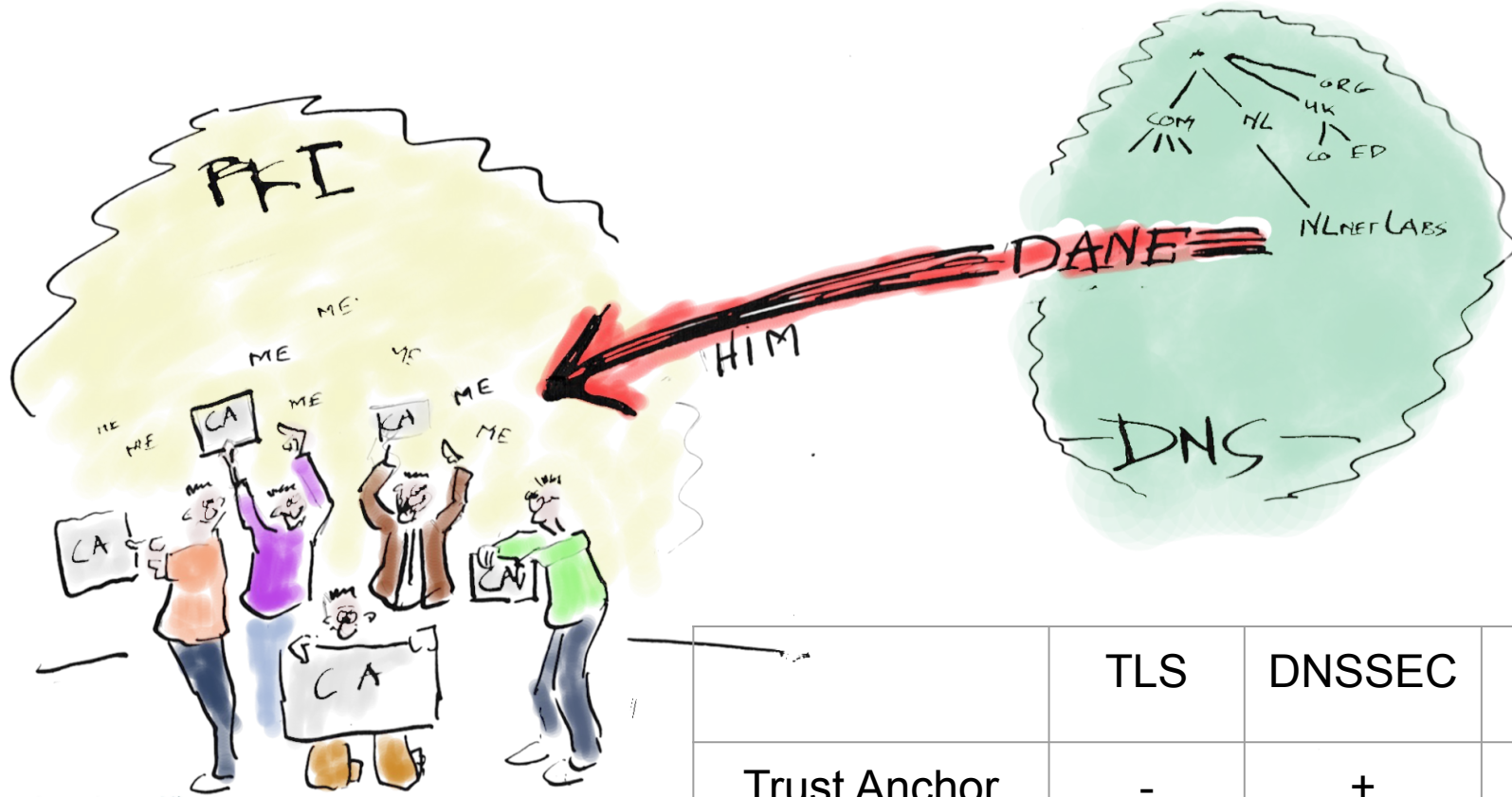
TLS, DNSSEC en RPKI - evaluatie



spotprent van Kloot

	TLS	DNSSEC	RPKI
Trust Anchor	-	+	+ -

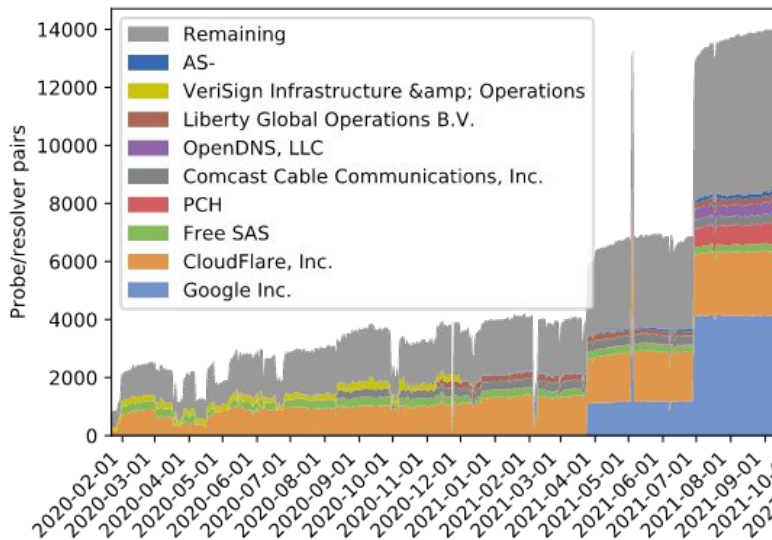
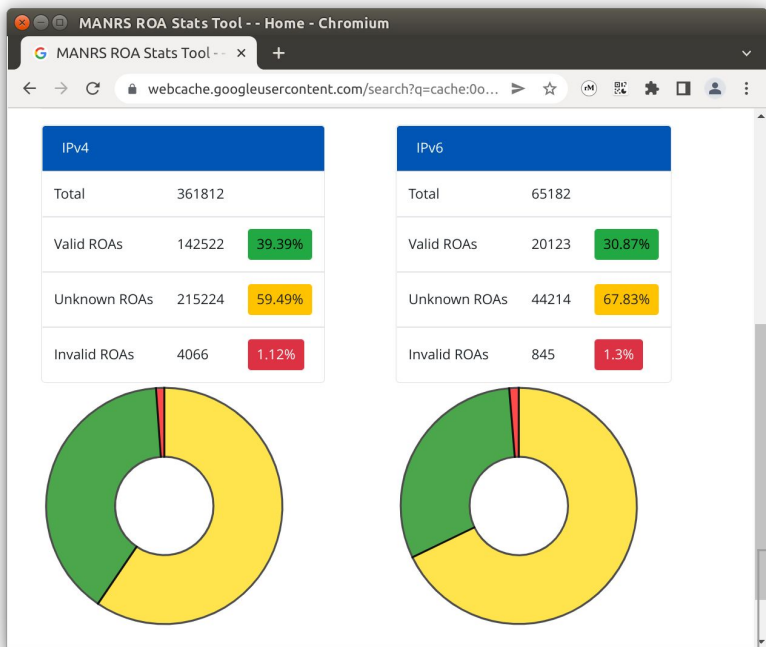
TLS, DNSSEC en RPKI - evaluatie



spotprent van Kloot

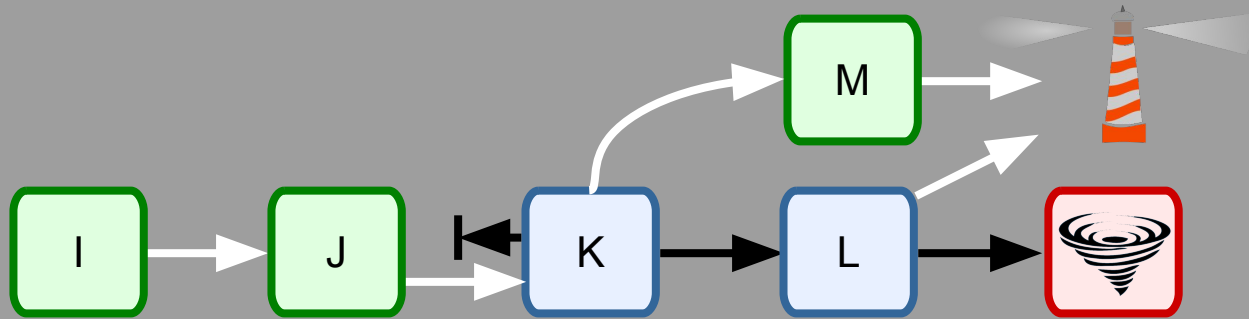
	TLS	DNSSEC	RPKI
Trust Anchor	-	+	+ -

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?