Hoe robuust is onze digitale overheid?

Raffaele Sommese[1] **Mattijs Jonker**[1]
Jeroen van der Ham[1,2] **Giovane C. M. Moura**[3,4]

1: Universiteit Twente **2**: NCSC **3**: SIDN Labs **4**:TU Delft

ECP Jaarfestival
Den Haag
2023-11-16

UNIVERSITY OF TWENTE.
Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid
SIDN LABS

Nederland: digitale ontwikkeling

Internet toegang	**97.8%**
Dagelijks gebruik Internet	**94.6 %**

bron: CBS.nl

Nederland: digitale overheid (e-gov)

RDW

Dienst Uitvoering Onderwijs
Ministerie van Onderwijs, Cultuur en Wetenschap

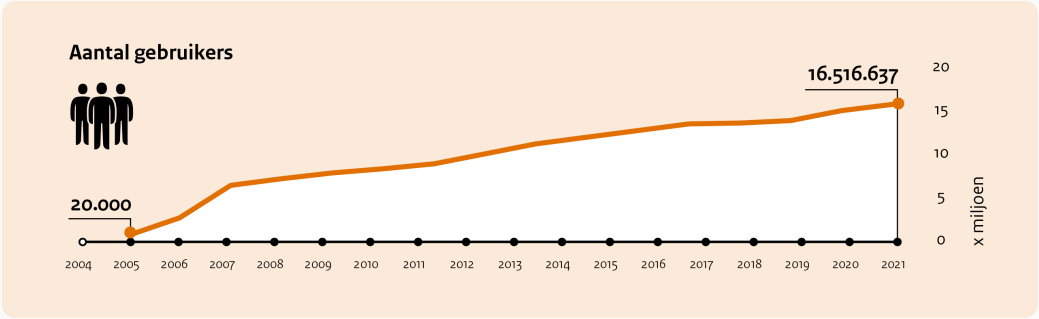
Belastingdienst

cbr

VREDE EN RECHT
Den Haag

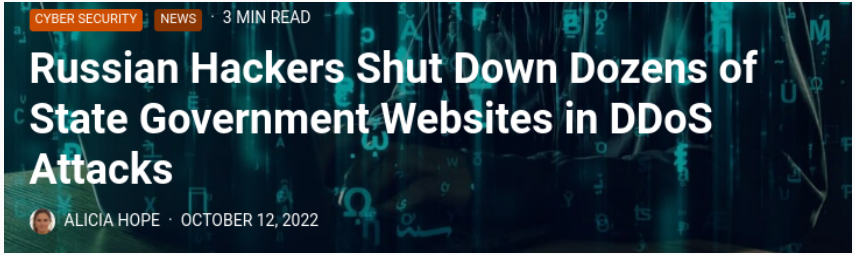
Reinier de Graaf

Nederland: digitale overheid (e-gov)



bron: Logius

Wanneer e-gov faalt...



bron: CPO Magazine

- Russische DDoS-aanvallen tegen verschillende Amerikaanse staten.
- Tijdelijke storing in e-gov Colorado, Connecticut, Kentucky, en Mississippi.

E-gov moet ook robuust zijn

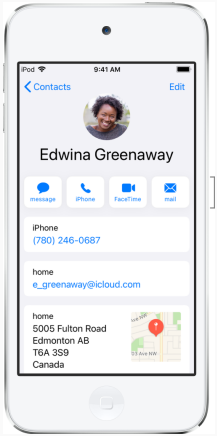
26 jaar oud Maeslantkering

bron: Rijkswaterstaat

Onze focus: DNS en e-gov betrouwbaarheid

Maar wat betekent DNS precies?

The Domain Name System (DNS)



Mensen

- `https://digid.nl`

Computers

- `144.43.243.208`
- We hebben moeite met het onthouden van nummers.
- DNS helpt ons.

Het Internet zonder DNS

E-gov DNS mag niet falen

bron: Unsplash

Opdracht: betrouwbaarheid van de Nederlandse e-gov-DNS

Opdrachtgever:

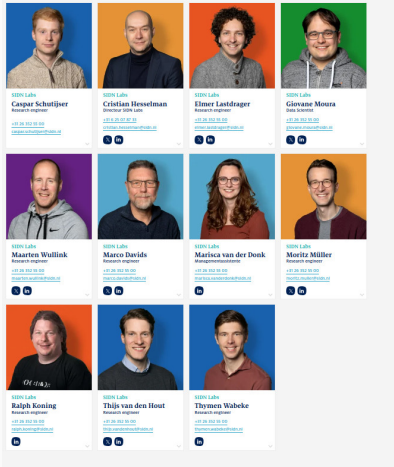
Uitvoerder:

Uitvoerder:

UNIVERSITY OF TWENTE.

Waarom SIDN Labs?

- SIDN is de `.nl` registry
  - veel ervaring met DNS
- SIDN Labs is het research afdeling
- Doel: verbeter de beveiliging van de internetinfrastructuur
  - focus op `.nl` en Nederland
- Wat we doen: grootschalige meetstudies, systeemontwerp, prototyping en evaluatie, bijdrage aan standaarden.
- Brug tussen de academische wereld en de operationele wereld/industrie.



SIDN Labs: DNS ervaring (RFC9199)

Independent Submission
Request for Comments: 9199
Category: Informational
ISSN: 2070-1721

G. Moura
SIDN Labs/TU Delft
W. Hardaker
J. Heidemann
USC/Information Sciences Institute
M. Davids
SIDN Labs

March 2022

Considerations for Large Authoritative DNS Server Operators

Abstract

Recent research work has explored the deployment characteristics and configuration of the Domain Name System (DNS). This document summarizes the conclusions from these research efforts and offers specific, tangible considerations or advice to authoritative DNS server operators. Authoritative server operators may wish to follow these considerations to improve their DNS services.

Waarom Universiteit Twente?

- Vakgroep @UTwente
- Richt zich o.a. op bestuderen en verbeteren van Internet veiligheid
- Veel ervaring met meten aan netwerken en analyse en fusie van grootschalige datasets

Het DINO project

- Het NCSC heeft een studie in opdracht gegeven met drie benodigdheden:
  - Inventariseren van aanbevelingen voor DNS beheerders en evaluatie naleving
  - Adviesrapport voor beleidsmakers en besluitvormers
  - Technisch verslag (vorm: peer-reviewed paper)
- In deze presentatie: hoofdbevindingen onderzoek

Betrouwebaar en robuust DNS

- In het DNS zit mogelijkheid voor robuuste configuratie
- Implementatie is niet altijd makkelijk en vereist middelen (o.a. financiële)
- Configuratieproblemen worden niet per se direct opgemerkt
  - Systeem werkt ogenschijnlijk tot het een dag stuk gaat (of gemaakt wordt)

Source: Unsplash

Hoofdvraag onderzoek

Is de DNS-infrastructuur voor Nederlandse overheiddiensten (e-gov) conform aanbevelingen geconfigureerd?

Aanpak: meetstudie

Hoofdvraag onderzoek

Is de DNS-infrastructuur voor Nederlandse overheiddiensten (e-gov) conform aanbevelingen geconfigureerd?

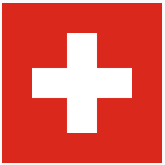
Aanpak: meetstudie

Onze contributies

1. Evaluatie voor Nederland en drie andere landen
    - via een meetstudie
2. Focus op Nederland, maar tevens in vergelijking met de andere landen
3. Aanbevelingen om het gebruik van het DNS door overheiddiensten te verbeteren

Nederland

Zwitserland



Zweden

Verenigde Staten

UNIVERSITY OF TWENTE.

Datasets

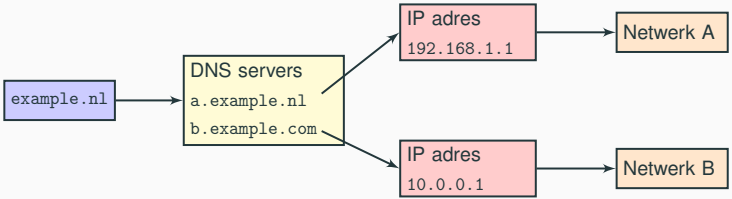
Land	Nederland .nl 	Zweden .se 	Zwitserland .ch 	Verenigde Staten .gov 
Domeinnamen (e-gov)	602	614	3971	7972
Populatie (land)	17.4M	10.4M	8.7M	332.9M

Hoofdbevinding 1: Single Point of Failure (SPoF)

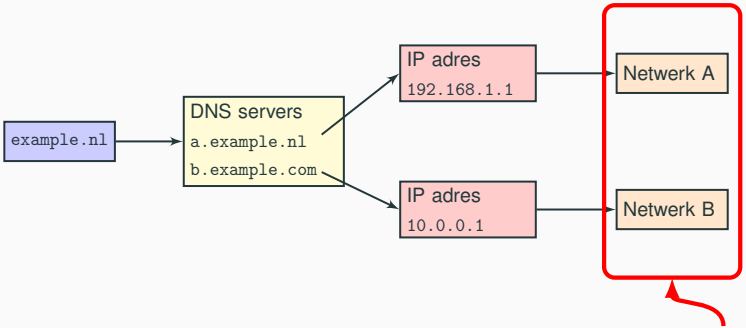
- Stop niet al je eieren in één mandje!
  - We kijken naar twee mandjes

Source: Unsplash

Eerste SPoF: enkele DNS-aanbieder



Eerste SPoF: enkele DNS-aanbieder



Unieke netwerken ∼ twee DNS-aanbieders

Eerste SPoF: enkele DNS-aanbieder

	Nederland	Zweden	Zwitserland	Verenigde Staten
domeinnamen	602	614	3971	7972
Reageert	601	609	3546	7911
enkele aanbieder (v4/v6)	43% /55%	41%/41%	43%/54%	82%/ 55%

- **VS: $\sim$ 80% enkele DNS-aanbieder (foei!)**

“Maar deze metriek is bogus!”

- “Ik stop alles wel in de **cloud**”
- Maar zelfs clouds kunnen falen
  - Dyn 2016
  - AWS Route 53 - 2019
- Zelfs Amazon.com gebruikt AWS niet voor DNS:

```
pdns1.ultradns.net.
ns4.p31.dynect.net.
ns2.p31.dynect.net.
pdns6.ultradns.co.uk.
ns1.p31.dynect.net.
ns3.p31.dynect.net.
```

“Maar deze metriek is bogus!”

- “Ik stop alles wel in de **cloud**”
- Maar zelfs clouds kunnen falen
  - Dyn 2016
  - AWS Route 53 - 2019
- Zelfs Amazon.com gebruikt AWS niet voor DNS:

```
pdns1.ultradns.net.
ns4.p31.dynect.net.
ns2.p31.dynect.net.
pdns6.ultradns.co.uk.
ns1.p31.dynect.net.
ns3.p31.dynect.net.
```

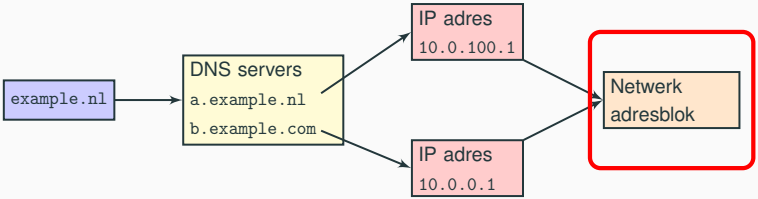
Centralisatie DNS-aanbieders: over wie hebben we het?

Nederland		Zweden		Zwitserland		Verenigde Staten	
netwerk	e-gov	netwerk	e-gov	netwerk	e-gov	netwerk	e-gov
TransIP	112	Loopia	47	Infomaniak	278	GoDaddy	1215
CLDIN	39	Tele2	23	Swisscomm	115	Cloudflare	909
QSP	28	Microsoft	21	Novatrend	100	Amazon	676
Solvinity	8	Telia	21	Abraxas	97	Akamai	334
SSC-ICT	8	Telia	19	Metanet	91	Tiggee	316

Table 1: Top 5 DNS-aanbieders for overheidsdiensten

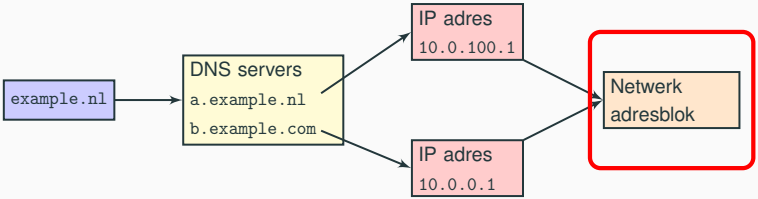
Meeste DNS-aanbieders zijn **lokaal**

Tweede SPoF: onderliggende netwerkinfrastructuur



- Als twee DNS servers in hetzelfde adresblok zitten (ongeacht aanbieder), zijn ze topologisch niet divers
- Ze delen de onderliggende netwerkinfrastructuur
  - Analogie: president en vice president wonen in hetzelfde huizenblok (en er valt een meteoor)

Tweede SPoF: onderliggende netwerkinfrastructuur

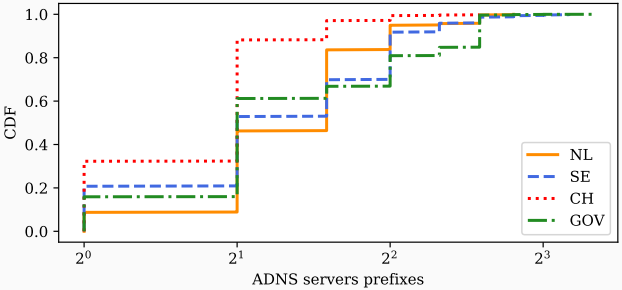


Zelfde adresblok $\sim$ zelfde lokatie

- Als twee DNS servers in hetzelfde adresblok zitten (ongeacht aanbieder), zijn ze topologisch niet divers
- Ze delen de onderliggende netwerkinfrastructuur
  - Analogie: president en vice president wonen in hetzelfde huizenblok (en er valt een meteoor)

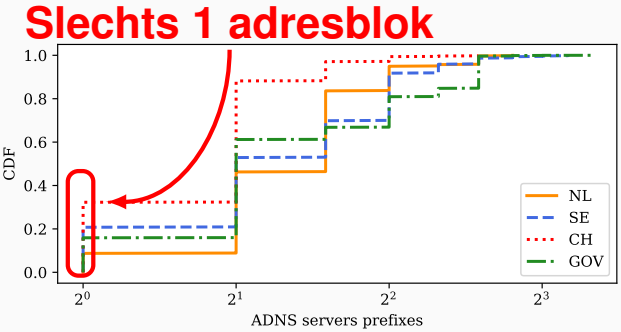
Tweede SPoF: onderliggende netwerkinfrastructuur

- Zwitserland: 1/3 e-gov domeinnamen zitten in hetzelfde adresblok
- NL, SE, US: $<$ 20%



Tweede SPoF: onderliggende netwerkinfrastructuur

- Zwitserland: 1/3 e-gov domeinnamen zitten in hetzelfde adresblok
- NL, SE, US: $<$ 20%



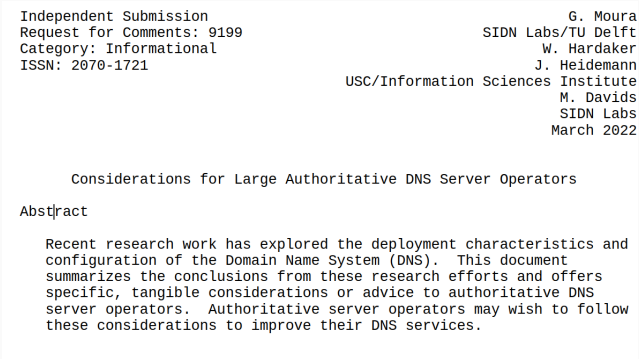
Extra weerbaarheid (RFC9199)

1.IP Anycast

- Behandeld in Moura16b

2.DNS Time-to-live (TTLs)

- Behandeld in Moura18b, Moura19b



Independent Submission
Request for Comments: 9199
Category: Informational
ISSN: 2070-1721

G. Moura
SIDN Labs/TU Delft
W. Hardaker
J. Heidemann
USC/Information Sciences Institute
M. Davids
SIDN Labs

March 2022

Considerations for Large Authoritative DNS Server Operators

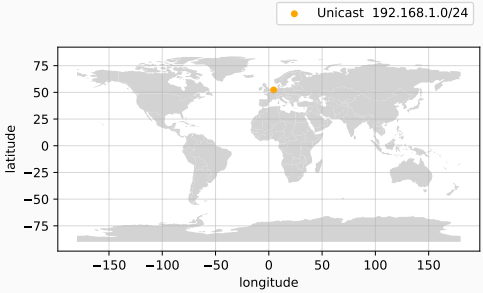
Abstract

Recent research work has explored the deployment characteristics and configuration of the Domain Name System (DNS). This document summarizes the conclusions from these research efforts and offers specific, tangible considerations or advice to authoritative DNS server operators. Authoritative server operators may wish to follow these considerations to improve their DNS services.

Beide behandeld in RFC9199

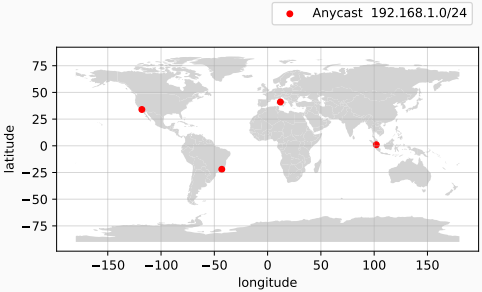
IP anycast

Unicast



- Ëën lokatie
- Bestemming van al het netwerkverkeer

Anycast

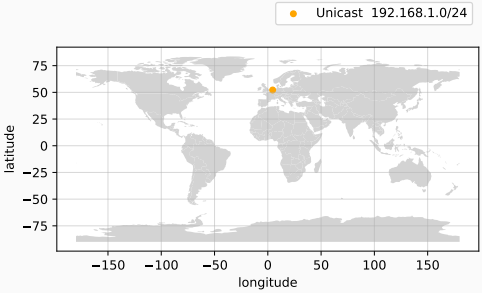


- Meerdere lokaties
- Netwerkverkeer wordt verdeeld

Anycast creëert weerbaarheid tegen aanvallen (Moura16b)

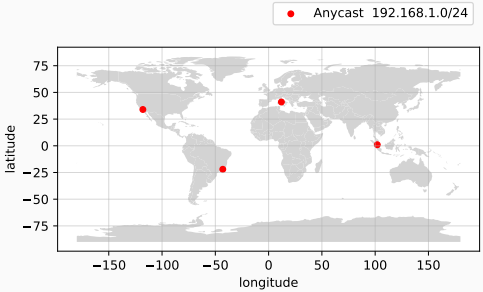
IP anycast

Unicast



- Ëën lokatie
- Bestemming van al het netwerkverkeer

Anycast

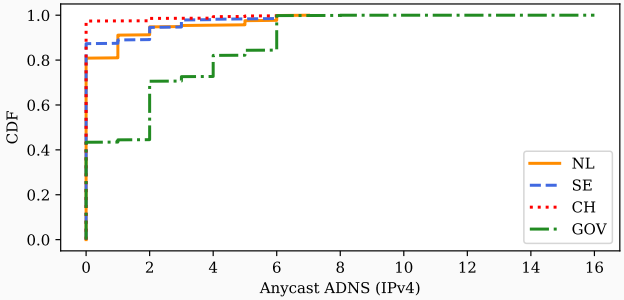


- Meerdere lokaties
- Netwerkverkeer wordt verdeeld

Anycast creëert weerbaarheid tegen aanvallen (Moura16b)

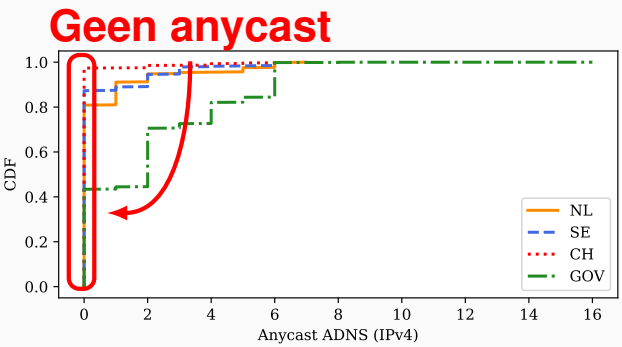
IP anycast onder overheidsdiensten

- Goed: 58% VS `.gov` overheidsdiensten gebruiken anycast
- Minder goed: zeer laag onder Zwitserse e-gov namen
- Zweden en Nederland rond 20%



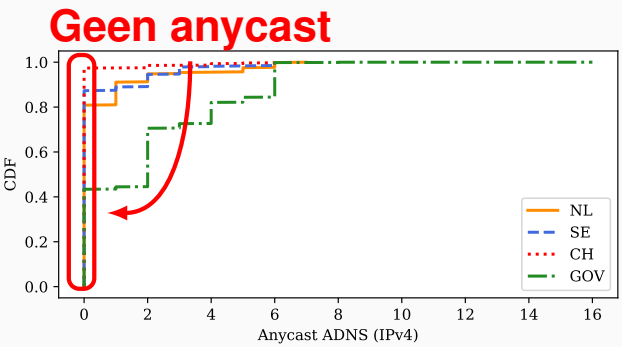
IP anycast onder overheidsdiensten

- Goed: 58% VS `.gov` overheidsdiensten gebruiken anycast
- Minder goed: zeer laag onder Zwitserse e-gov namen
- Zweden en Nederland rond 20%



IP anycast onder overheidsdiensten

- Goed: 58% VS `.gov` overheidsdiensten gebruiken anycast
- Minder goed: zeer laag onder Zwitserse e-gov namen
- Zweden en Nederland rond 20%



Aanbevelingen voor overheidsdiensten

- **Diversificeer:** meer DNS-aanbieders (of beheerders)
- **Gebruik** anycast voor (extra) weerbaarheid
- **Heroverweeg** lagere TTL waarden

Robuust (1900 jaren oud) infrastructuur in Segovia, Spanje. Bron: Wikipedia

Conclusies

- Veel overheidsdiensten leven aanbevelingen voor robuuste DNS configuratie niet na
- Dit leidt tot een onnodig risico voor falen
- We hopen dat onze bevindingen ertoe leiden dat de robuustheid en weerbaarheid wordt verbeterd

Robuust (1900 jaren oud) infrastructuur in Segovia, Spanje. Bron: Wikipedia

Technisch verslag: Sommese22a