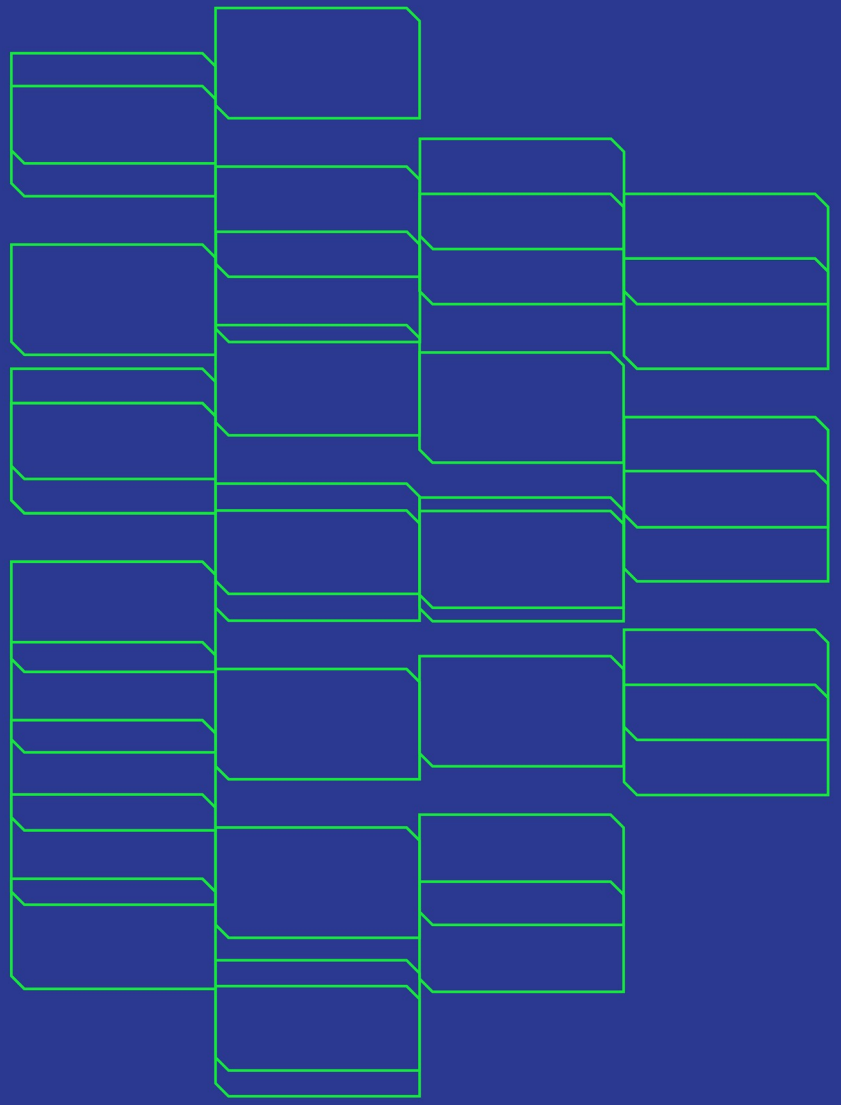
Security .Days

<Utrecht.NL>
<7-9 April 2026>

GÉANT

Protective DNS

Joeri de Ruiter (SURF)

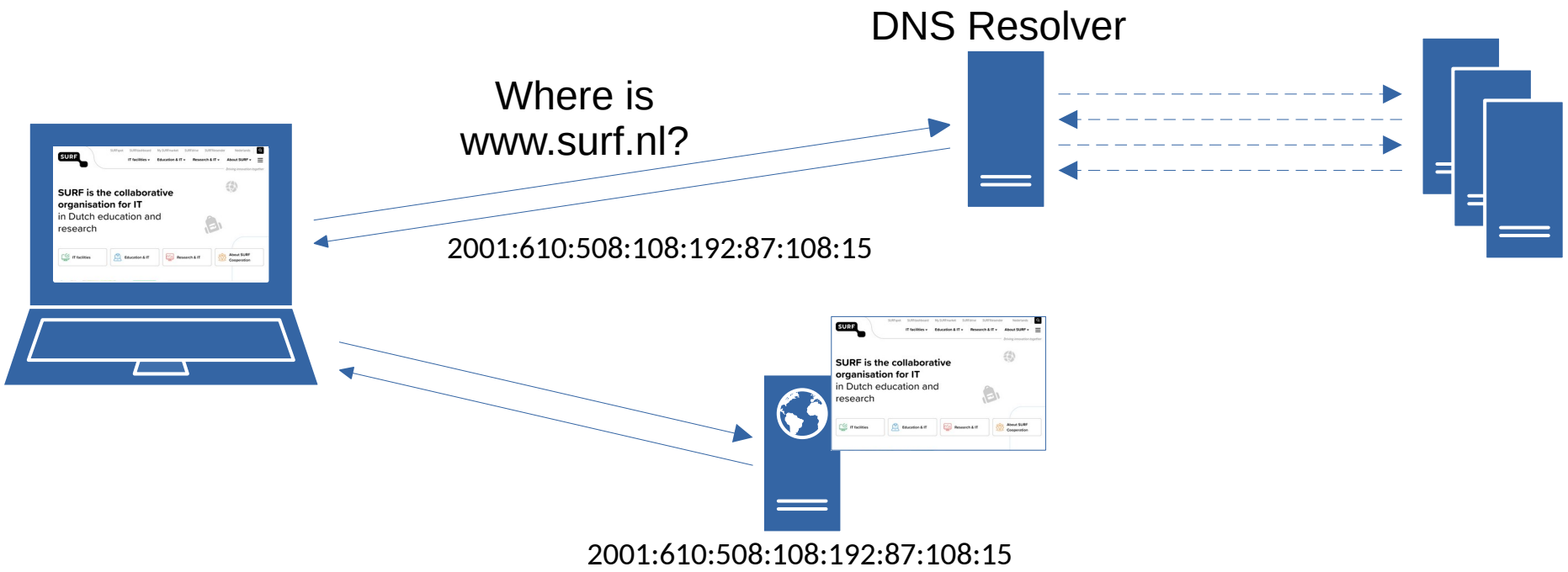


Co-funded by
the European Union

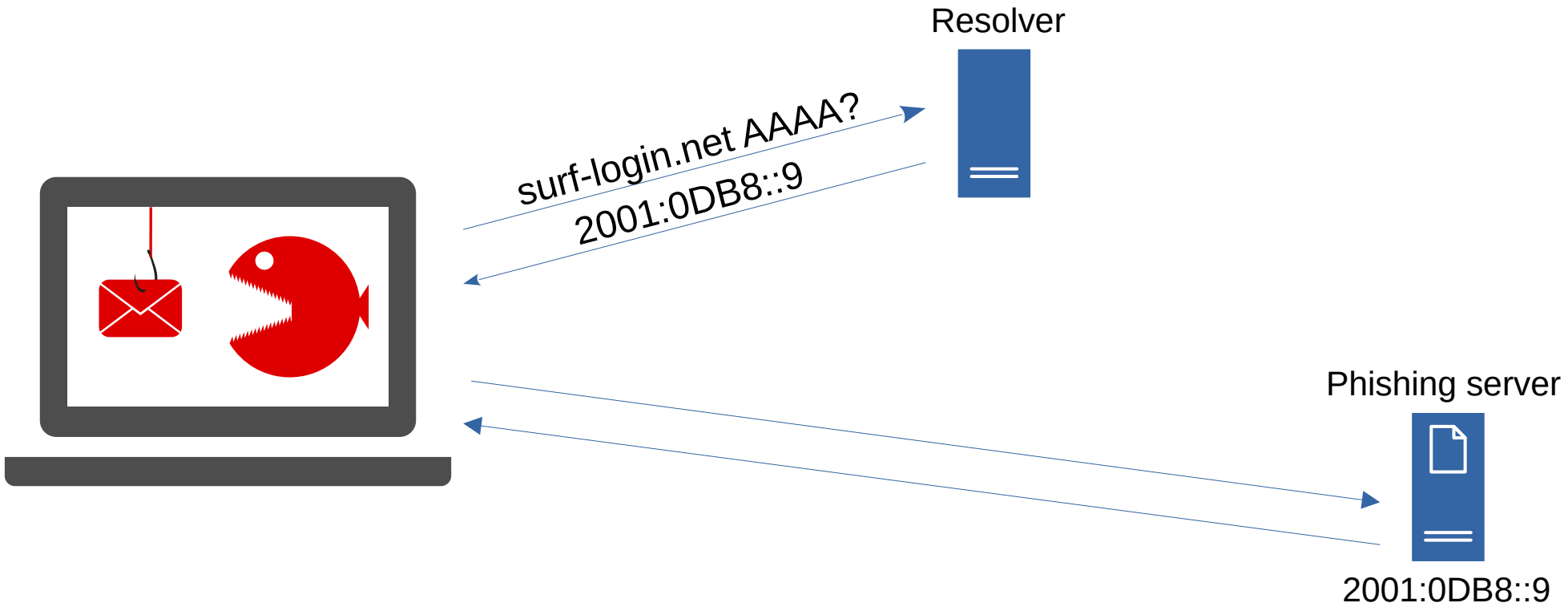
Protective DNS

- Subtask of GN5-2 WP8 Task 3 (Security Operations Tooling)
- Members from SUNET, GEANT and SURF
- Goals
  - Develop and deploy a pilot service
  - Provide a blueprint to deploy the service yourself

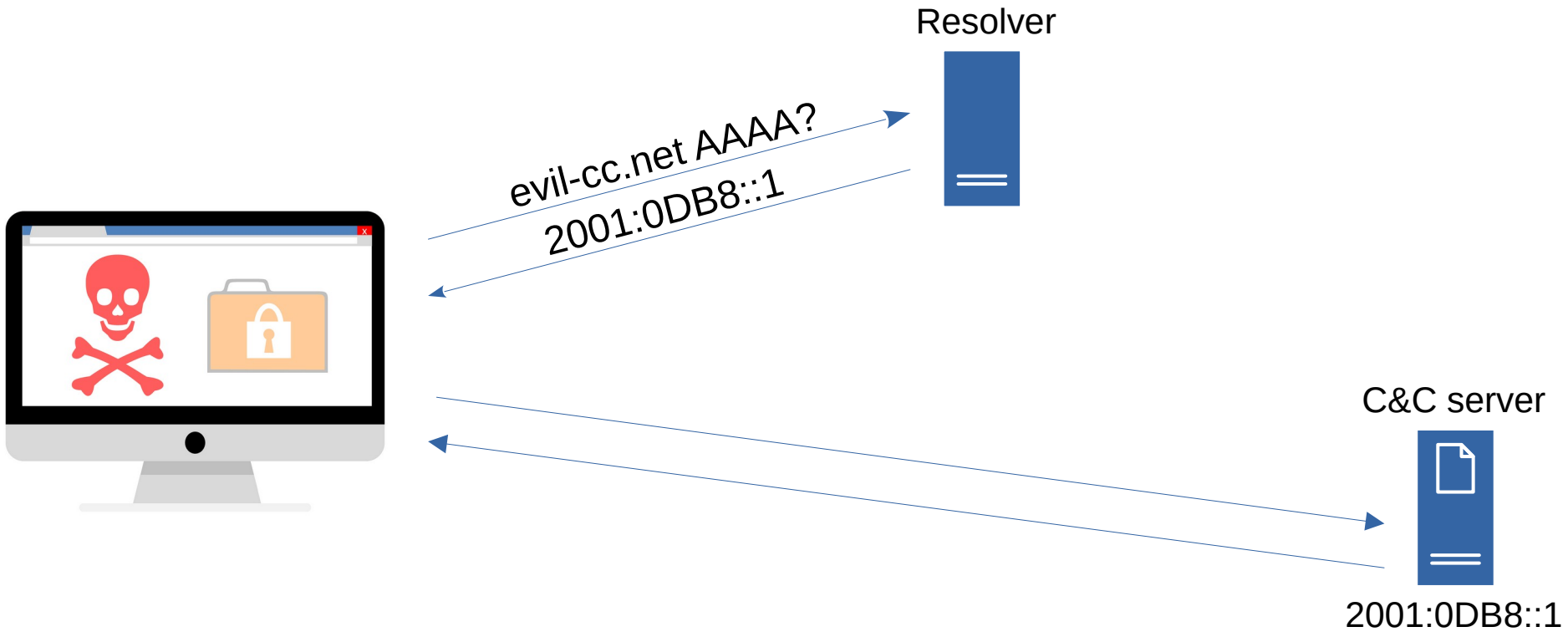
DNS (Domain Name System) intro



Phishing

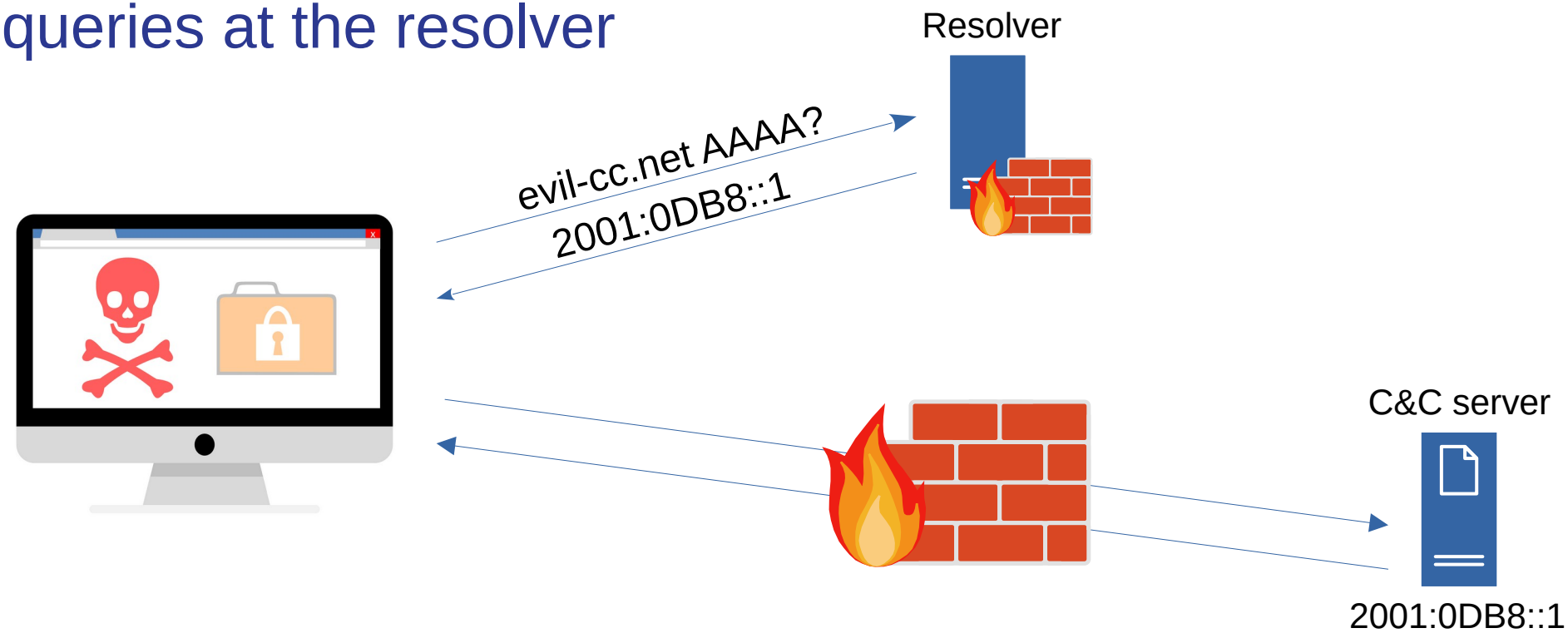

Resolver
surf-login.net AAAA?
2001:0DB8::9
Phishing server
2001:0DB8::9

Malware



Protective DNS

- Filter queries at the resolver



Response policy zones

- Regular DNS zones
- Block queries when matching
  - Query name
  - IP address in response
- Possible actions
  - No/empty answer (NXDOMAIN / NODATA / drop)
  - Redirect using CNAME (e.g. redirect to landingpage)
  - Passthru (allowlists)

Protective DNS setup

- Anycast
  - Nodes at different NRENs
- Blocking and resolving split
- When domain is blocked NXDOMAIN is returned (not found)
  - EDE (Extended DNS Errors) use to indicate blocking

Logging

- DNS queries reveal user’s browsing behaviour
- Only hits logged
- IP address reduced to /24 or /48
- Institutional level and not individual users

Protective DNS setup

```
$ dig @145.98.16.1 testentry.rpz.threatfox.abuse.ch

...

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 61393

;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1


;; OPT PSEUDOSECTION:

; EDNS: version: 0, flags:; udp: 1232

; EDE: 15 (Blocked): (This domain was blocked by the ProtectiveDNS service)

;; QUESTION SECTION:

;testentry.rpz.threatfox.abuse.ch. IN    A
```

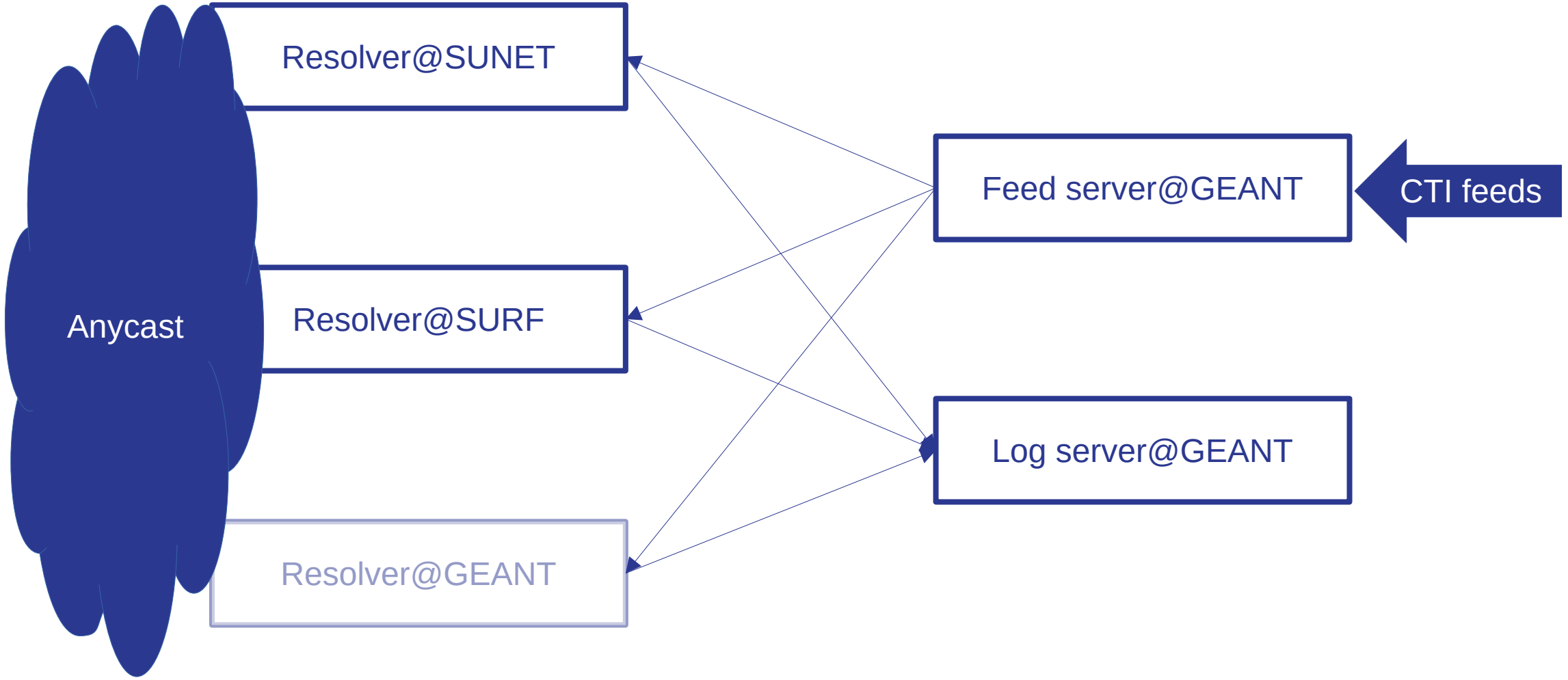
Blocking

- Blocklists
  - Collaboration with CTI task
  - Comparison between different feed providers
- Allowlists
  - Possible to prevent blocking of important domains

Protective DNS architecture

- Resolver
  - Filtering: dnsdist
  - Resolving: Unbound
- Feed distribution
  - rsync
- Logging
  - DNSTAP

Protective DNS architecture



Protective DNS service

- **Join us!**
- Operational on address 145.98.16.1 (anycast)
- Best effort
  - With monitoring
- Contact us if you want to use it
  - https://wiki.geant.org/spaces/G52W8/pages/1307869228/Service+description

What do you want?

- Blueprint to run the service yourself or a complete running service?
- What kind of logging and statistics would you like to see?
  - How would you want to receive them?
- When blocking: NXDOMAIN or landingpage or …?
- Are there other features you would like to see?
- ...

Questions?

joeri.deruiter@surf.nl

Co-funded by
the European Union