# Private Relay Services

## Localization of traffic –
## Does it really work?

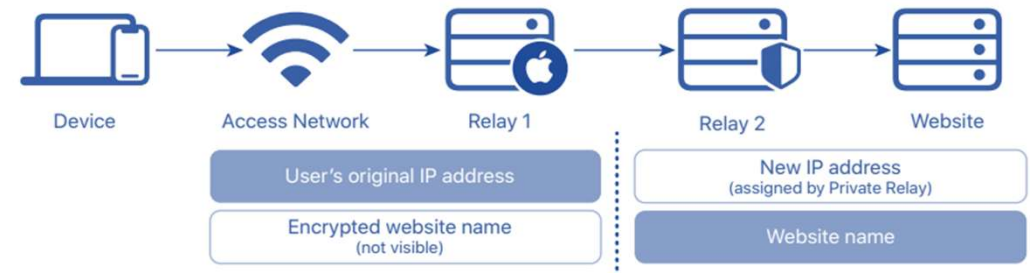2023

# Background on Private Relay

# Acknowledgement

o   Private Relay traffic has, by design, its limitations with regards to traffic analysis even though the architecture is well documented

o   Based on our research and findings, only Safari- and port-80 traffic is currently handled over Private Relay. This is not necessarily a representative traffic profile

o   Special thanks to Patrick Sattler from Technical University of Munich for advice and research data

# Architecture

The prominent design feature in this private relay service is the ingress/egress-proxy structure:

- It secures that no party in the chain can connect source & destination, not even the proxy providers
- Ingress Proxies are operated by Apple (some hosted by Akamai)
- Egress Proxies are operated by Akamai, Cloudflare or Fastly

**Private Relay Dual-hop Architecture**



Device → Access Network → Relay 1 → Relay 2 → Website

| User's original IP address | New IP address (assigned by Private Relay) |
| Encrypted website name (not visible) | Website name |

Source: apple.com/privacy/docs/iCloud_Private_Relay_Overview_Dec2021.PDF
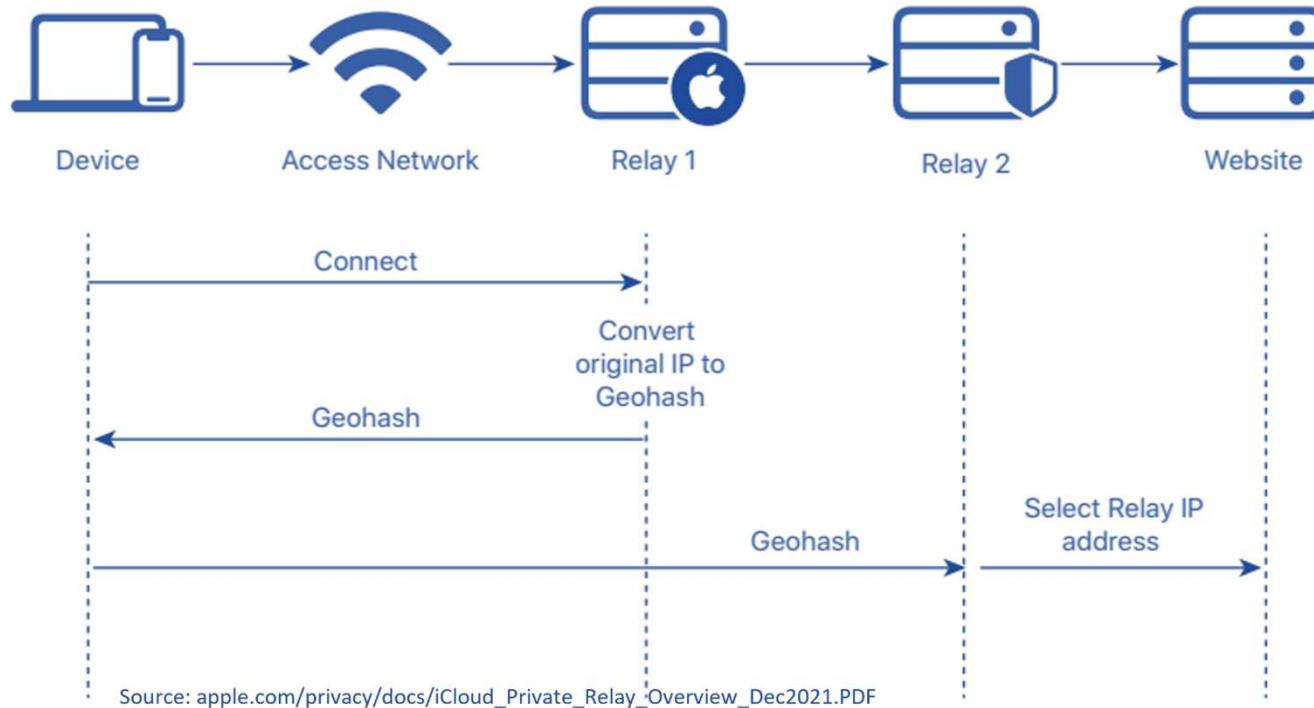
# Localization challenge



Device → Access → Relay 1 → Relay 2 → Website

CDN's try to localize traffic as close to the end-user as possible. This becomes challenging for two reasons:

- In Private Relay, CDNs have limited visibility on end-users' location
- Relay-1 (aka Ingress-Proxy) is handing over the content to the access-network. Geographical spread of these proxies might not resemble major CDN's server- and interconnect footprint.

# Solution-1 for localization challenge: Geo-Hashing



Device     Access Network     Relay 1     Relay 2     Website

Connect

Convert original IP to Geohash

Geohash

Select Relay IP address

Geohash

Relay-1 provides a geo-hash which translates into a geo-representative IP for Relay-2

# Solution-2 : Edge locations for Relay-1



AS36183 (Akamai-AS used for iCloud private relay) announces ~550 x /24

o  This could be an indication for the number of locations for Relay-1
o  Fairly good coverage, but surely less than the typical footprint of major CDNs

# Our Findings

# What BENOCS does
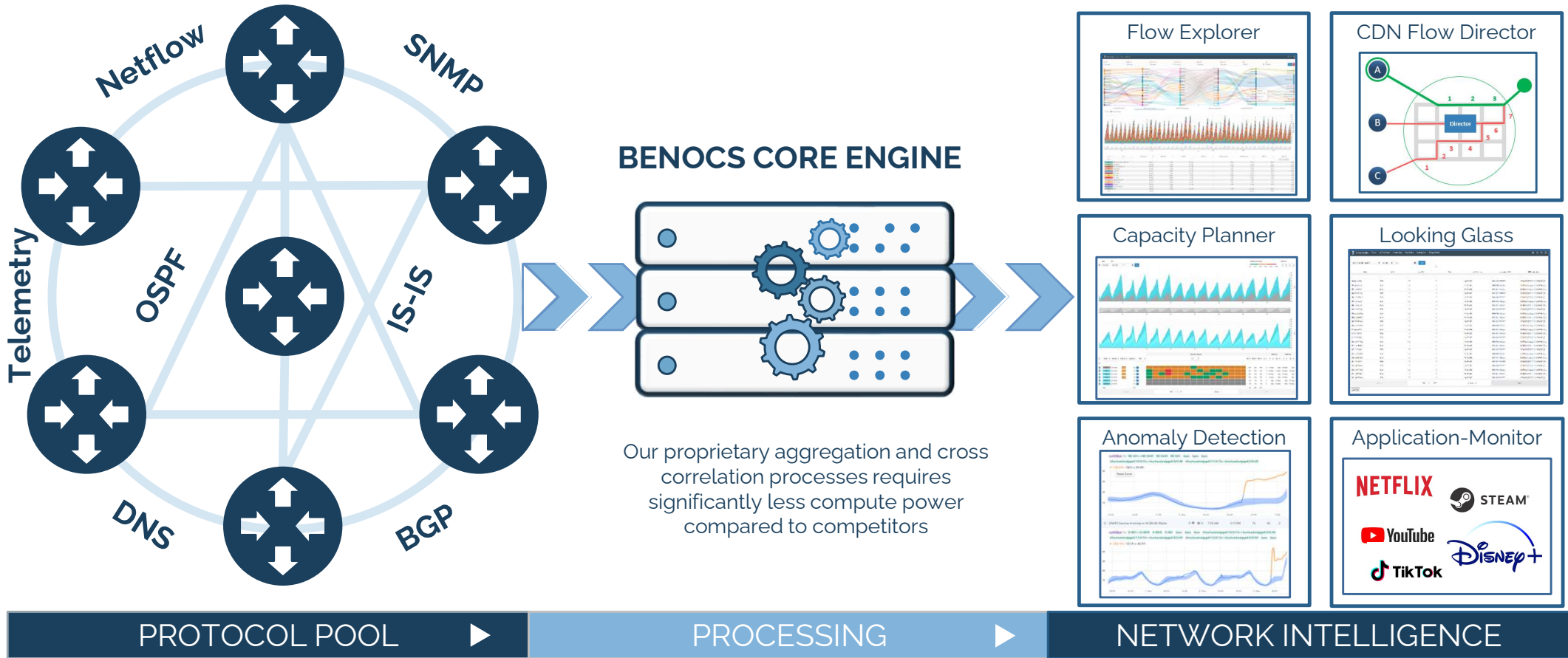


**BENOCS CORE ENGINE**

Our proprietary aggregation and cross correlation processes requires significantly less compute power compared to competitors

Netflow

SNMP

Telemetry

OSPF

IS-IS

DNS

BGP

Flow Explorer

CDN Flow Director

Capacity Planner

Looking Glass

Anomaly Detection

Application-Monitor

NETFLIX
STEAM
YouTube
Disney+
TikTok

PROTOCOL POOL ▶ PROCESSING ▶ NETWORK INTELLIGENCE
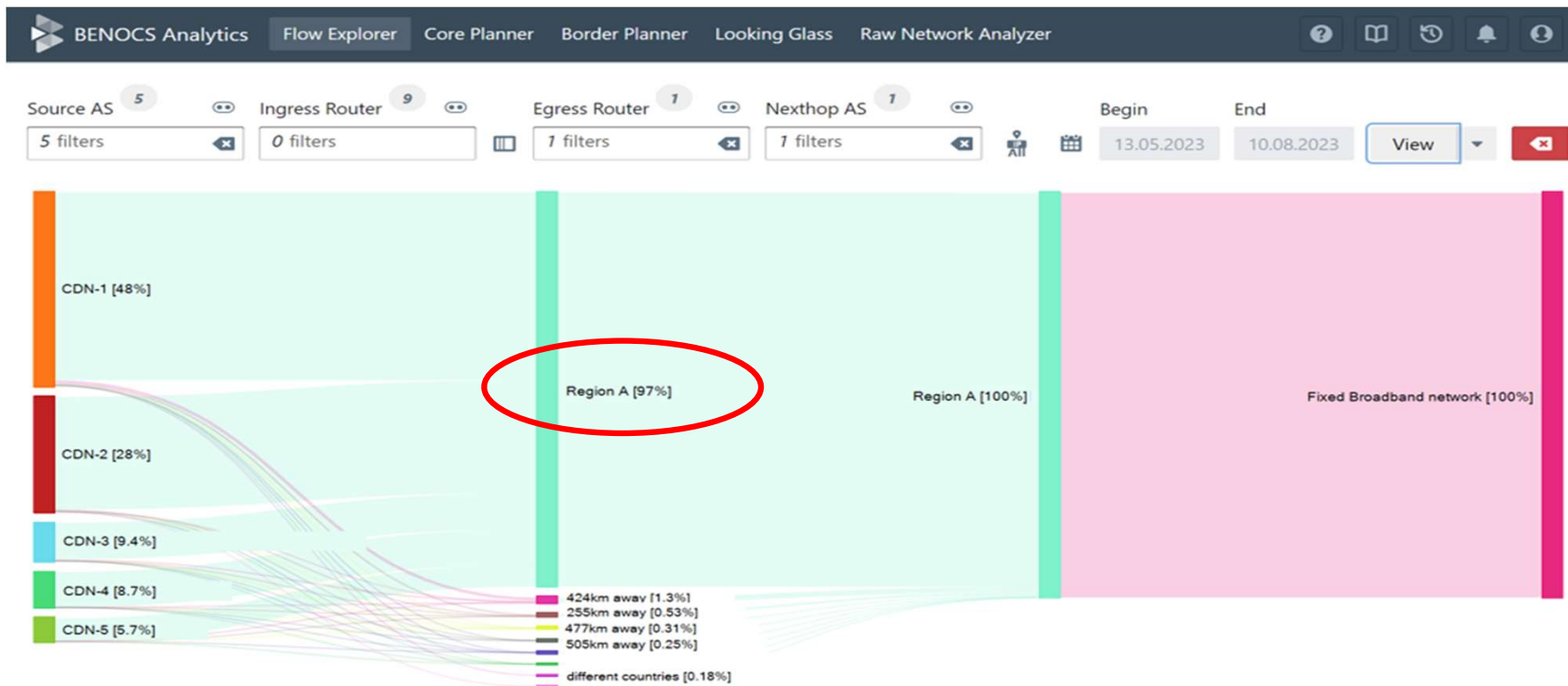
BENOCS

# Our Methodology

*We compared the "ingress-distance" between 5 major CDNs and Private-Relay IP's for a representative region in a larger access network*

- o Split between fixed-broadband and mobile
- o Over 90 days
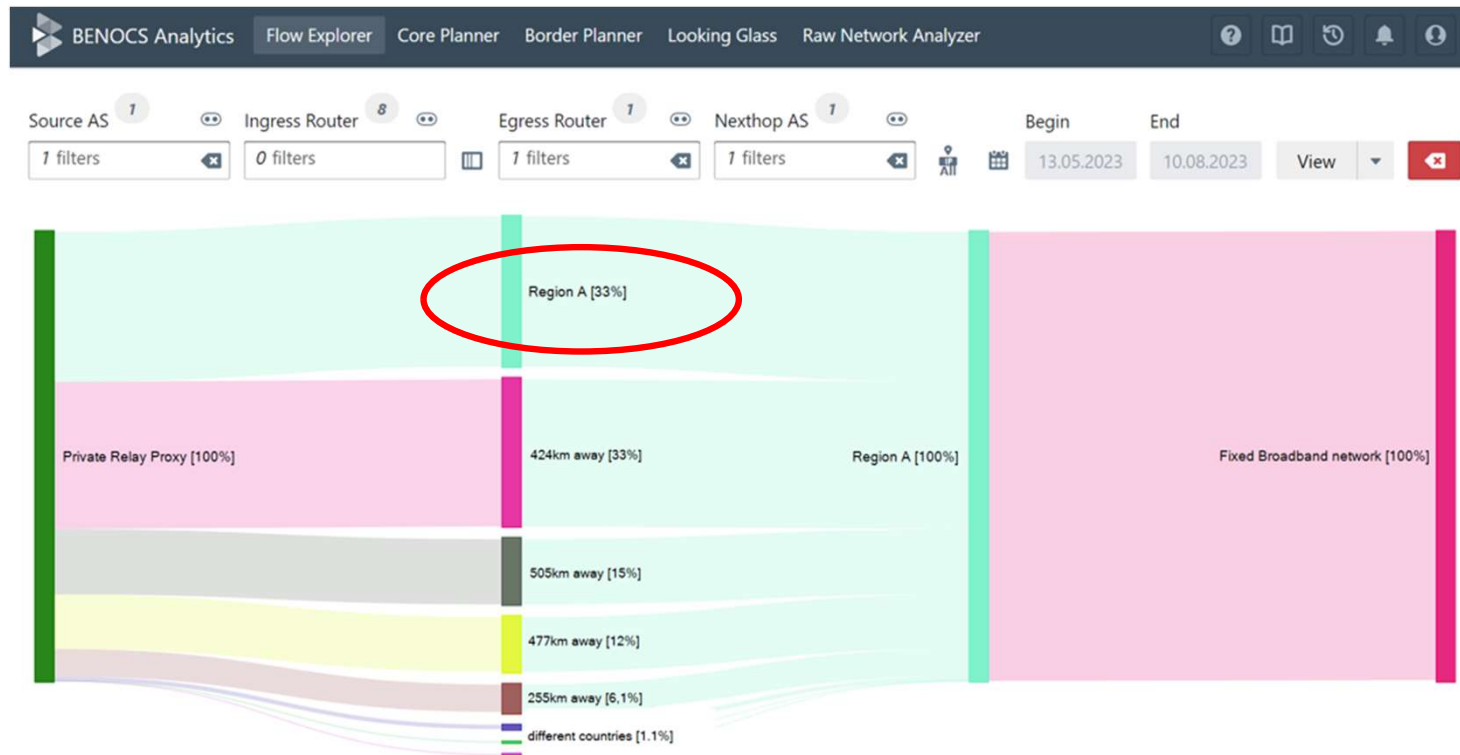- o All following traffic data is from BENOCS Analytics
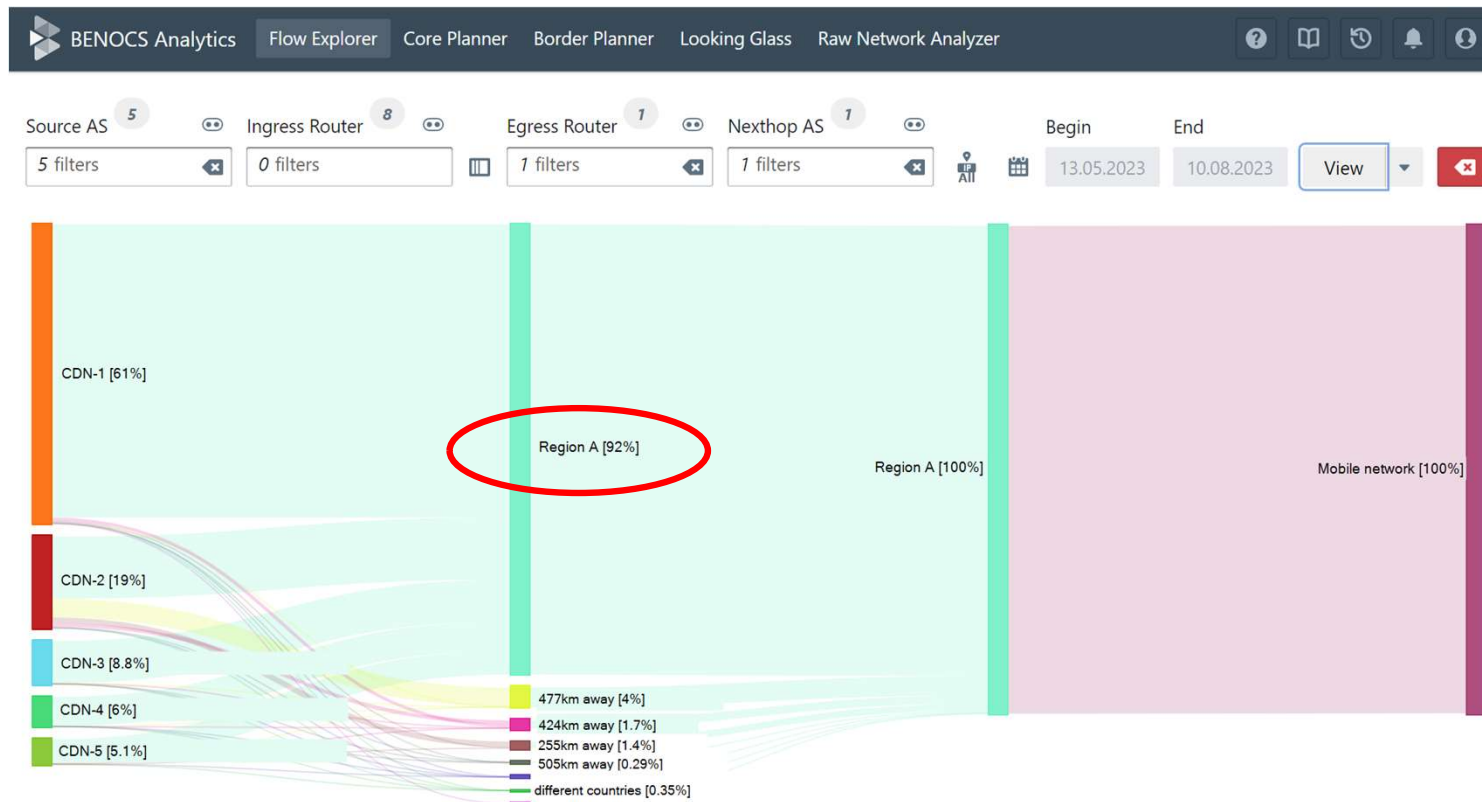
# What does an access network see?
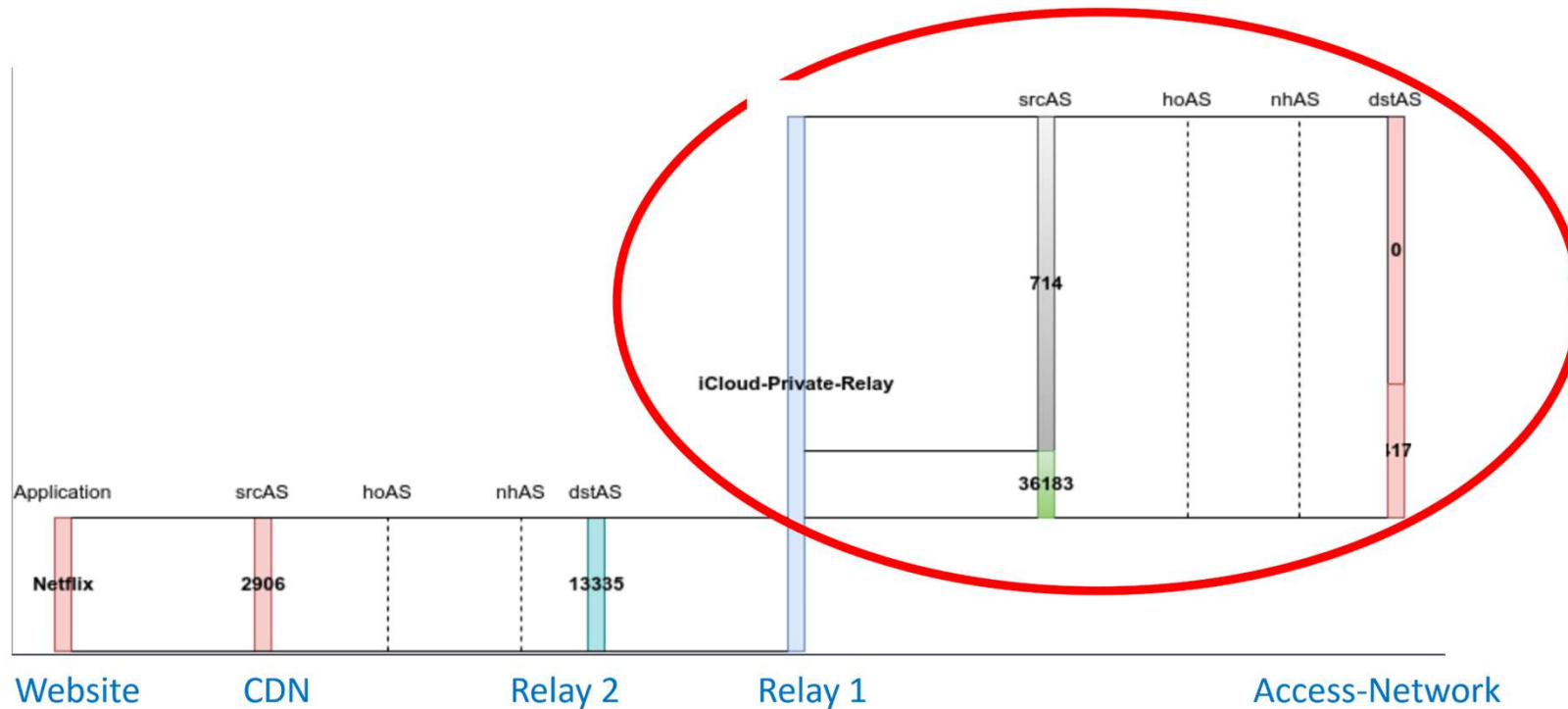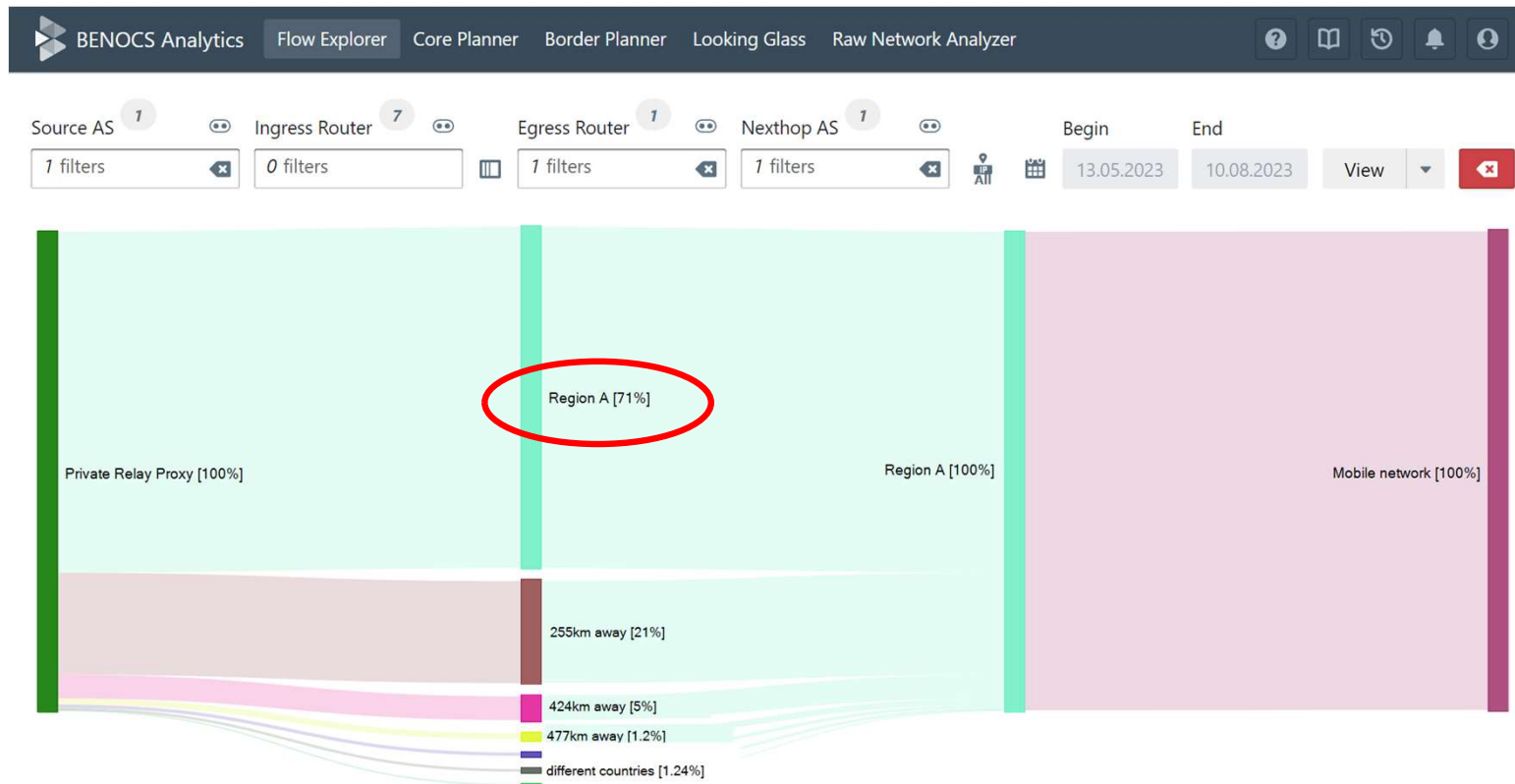
# Benchmark: 5 CDN localization - fixed

# Result: Private Relay localization - fixed

# Benchmark: 5 CDN localization - mobile

# Result: Private Relay localization - mobile

# Our Conclusion

## *Localization in private relay networks is not fully effective*

Potential reasons:

- Mapping via geo-hash depends on quality of geo-data

- Geo-distance does not always equal network distance

- Volatility in localization: capacity/availability issues?

- Data might not be representative - Traffic levels are low, traffic profile is limited

BENOCS

# Stephan Schroeder

sschroeder@benocs.com

BENOCS GmbH

Reuchlinstr. 10, 10553 Berlin

+49 30 577 000 4 – 0

**benocs.com**



# Thank you!

# Questions?