TF-CSIRT/FIRST TC Team update

UNINETT CERT

January 29th 2008

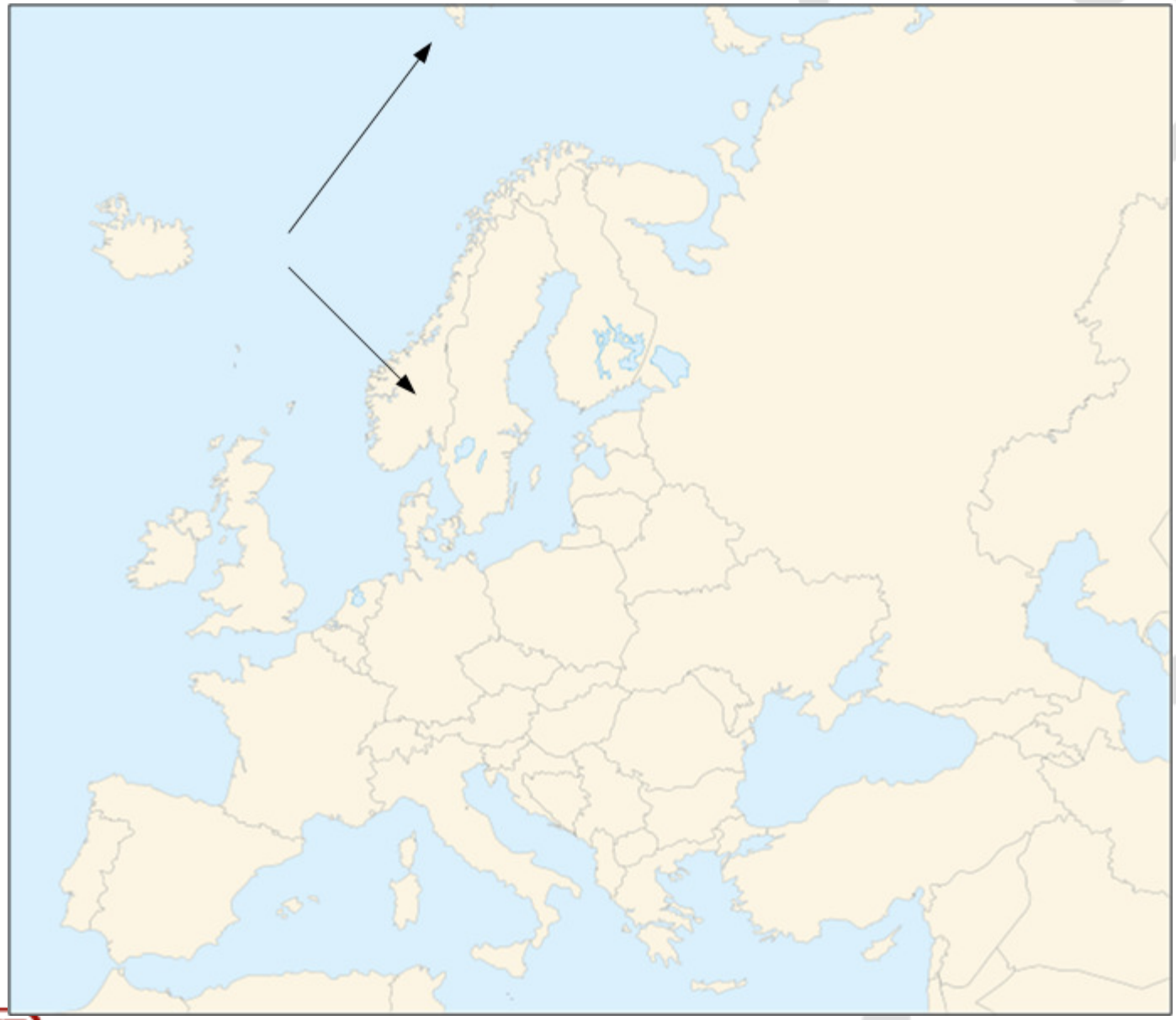
Per Arne Enstad

UNINETT? What? where?

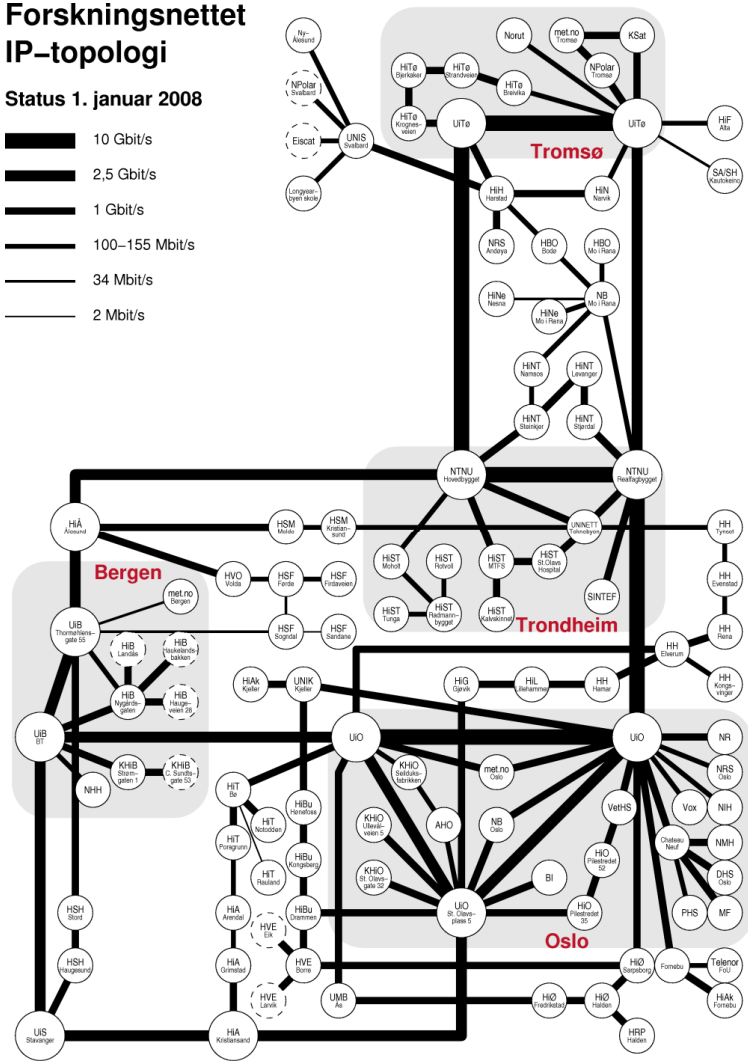
- UNINETT develops and operates the Norwegian national research network, which links together domestic educational and research institutions and connects them into international networks

UNINETT

- Serving 75+ customers
- Approx. 300 POPs
- Approx. 400K end users



Our main product:



UNINETT CERT

- Established 1995
- Constituency:
  - All customers within our address space
- Virtual team organized within the NOC
  - Core team: 4 persons working part time
- Member of FIRST since 2000
- TI Accredited Team since 2001

UNINETT CERT

- Work profile:
  - Incident prevention
    - Security audits
    - IRT-courses
    - Best practices
  - Incident handling
    - Mostly coordination, but still a few ”hands on” cases
    - Workload: approx 5000 incidents/year

UNINETT

UiO CERT

- University of Oslo is by far our largest customer
- Established 2002 but went dormant for various reasons
- Revitalized in 2006 and at this point:
  - TI Accredited Team Jan ’08
  - Core Team: 8 persons + access to other resources when required

UNINETT

Current development efforts

- Further RTIR-work
  - Extentions and integration
- Passive DNS monitoring
- Flow vizualisation
  - Ongoing masters thesis
- Anomaly detection
  - Testing techniques of varying complexity
- Child Sexual Abuse Anti-Distribution Filter

UNINETT

Current development efforts (2)

- Scripting and extending nfdump/nfsen
  - e.g. internal per-organization aggregation
- IPv6 flow collection

UNINETT

TF-CSIRT

- UiO CERT and UNINETT CERT will host the May ’08 meeting in Oslo
- Stay tuned on the TERENA website for details
- Welcome!

Questions?