O4.2-647

Secure Data Communication for Nuclear Monitoring at the Swedish NDC

Jon Grumer[1], Henrik Olsson[1], Marius Popa[2]

[1]FOI - Swedish Defence Research Agency
[2]CTBTO Preparatory Commission

12 September 2025

Introduction

- The waveform research activity at the Swedish NDC (FOI) has been relatively low since the early 90’s.
- Current reboot and capacity buildup
  ~1 fulltime staff for decades → 5-6 in seismology, geophysics & meteorology
- Modern waveform research puts new demands on **IT infrastructure security**

Introduction

- The waveform research activity at the Swedish NDC (FOI) has been relatively low since the early 90's.
- Current reboot and capacity buildup
  ca 1 fulltime staff for decades → 5-6 in seismology, geophysics & meteorology
- Modern waveform research puts new demands on **IT infrastructure security**

Key challenges

- Streaming data in **realtime** into secure network for further processing
  - Eg: realtime data = continuous exposure, persistent entry point for attackers
- Include CTBTO's Global Communications Infrastructure (GCI) network
- Facilitate seedlink/fdsnws server, open to other institutes/collaborators

Data protocols (SHI)

SeedLink – near-realtime waveform data, typically not encrypted

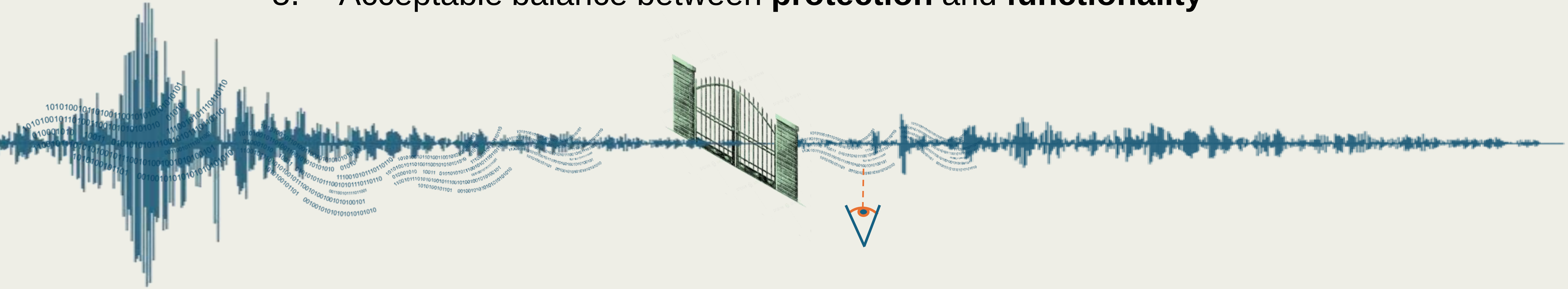
- Standard TCP/IP port 18000

FDSN Web Services – on-demand waveform and meta data, not encrypted

- RESTful web service interfaces

Requirements on data infrastructure

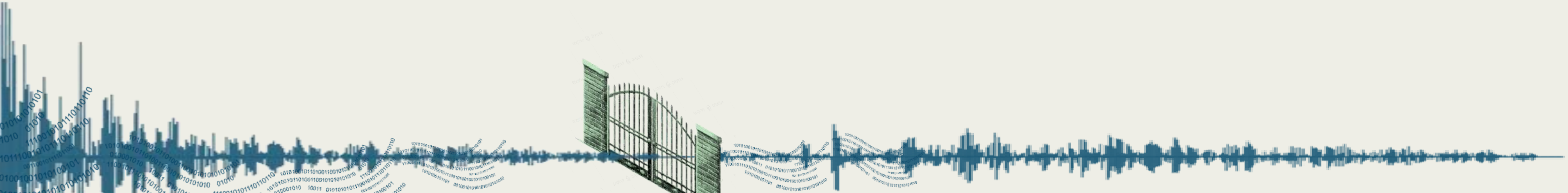
1. Data should be able to flow **in** and **out** - also in realtime (SeedLink)
2. **Monitoring** of data streams should be possible
3. **Gatekeepers** at various levels to limit network traffic
4. **Software** for receiving/transmitting data, including IMS
5. Acceptable balance between **protection** and **functionality**



Gatekeeping and monitoring

- Set up an intermediate server in an isolated, low-security network
- **Install necessary software**, including **CTBTO’s new software VPN**
- From this server, allow data streams to internal network – but how?
  - Encrypted data can’t easily be monitored
    – thus, tools such as **ssh portforward** does not fit the bill
  - Better: **reverse proxy** on intermediate server

- Collect all data sources in this proxy (realtime and on-demand)
- Firewall: e.g only allow connections to this proxy from inside the secure network - limit all other sensitive streams

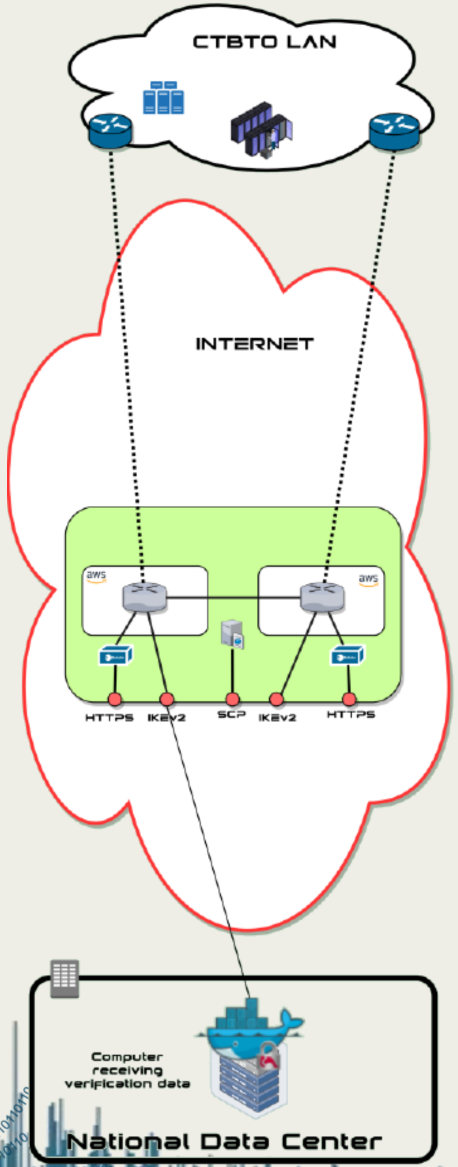


FOI Swedish Defence Research Agency

Jon Grumer, Henrik Olsson, Marius Popa (CTBTO)

O4.2-647

Docker VPN Cloud Solution



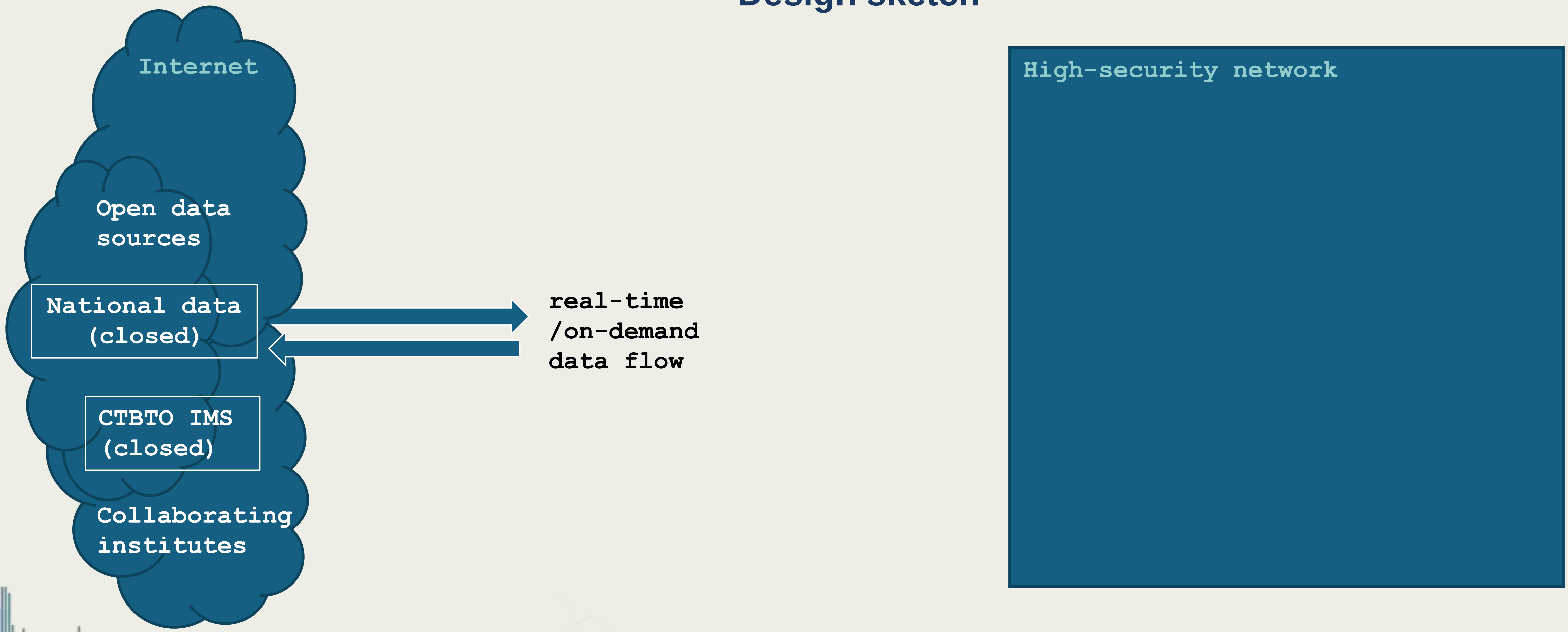
GCI VPN - the new software docker solution

In depth presentation: P4.2 "*Virtual GCI for NDC (VPN Docker)*"
Marius Popa, CTBTO Prep. Comm.

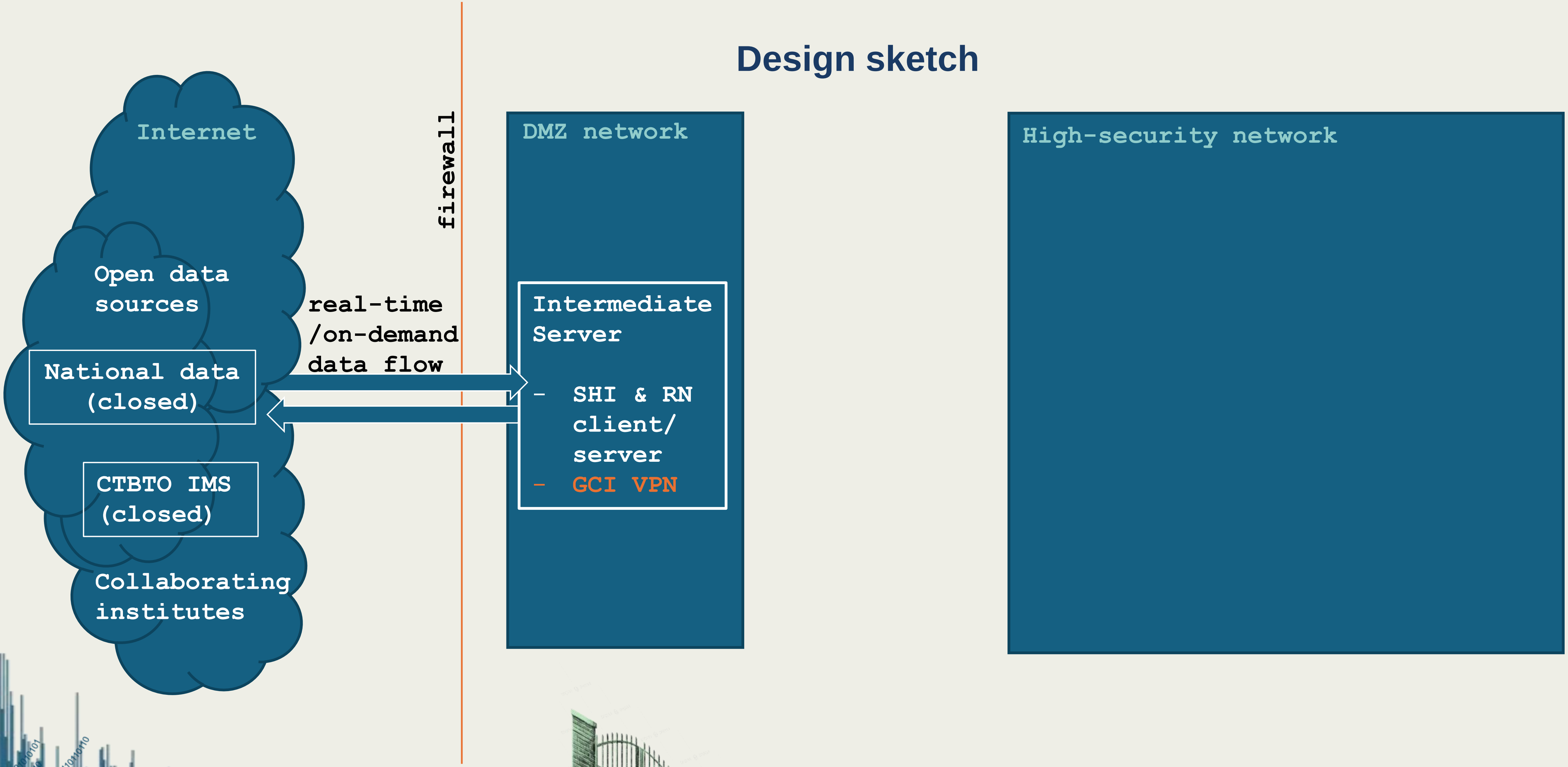
- **Why?** **-** Growing demand of data delivery to National Data Centres based on cloud infrastructures
- **What?** **-** A Linux Docker container running programmable VPN clients
- **Benefits?**
  - Flexible & fast deployment (~minutes)
  - Any Linux-based platform – ensuring latest security standards
  - Automated monitoring and alerting
  - Unique disaster recovery concept for robust communication

FOI Swedish Defence Research Agency

Design sketch



Design sketch



Internet

Open data sources

National data (closed)

CTBTO IMS (closed)

Collaborating institutes

real-time /on-demand data flow

firewall

DMZ network

Intermediate Server

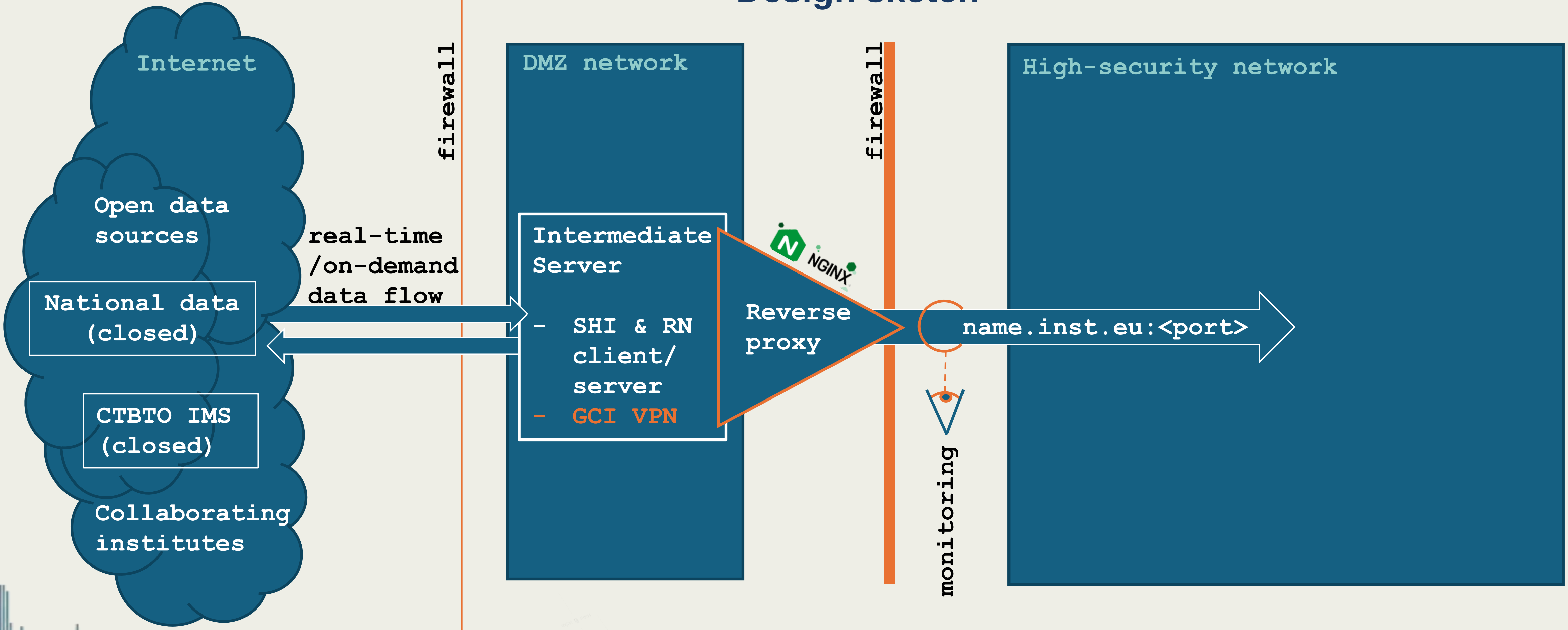
- SHI & RN client/ server
- GCI VPN

High-security network

Jon Grumer, Henrik Olsson, Marius Popa (CTBTO)

O4.2-647

Design sketch

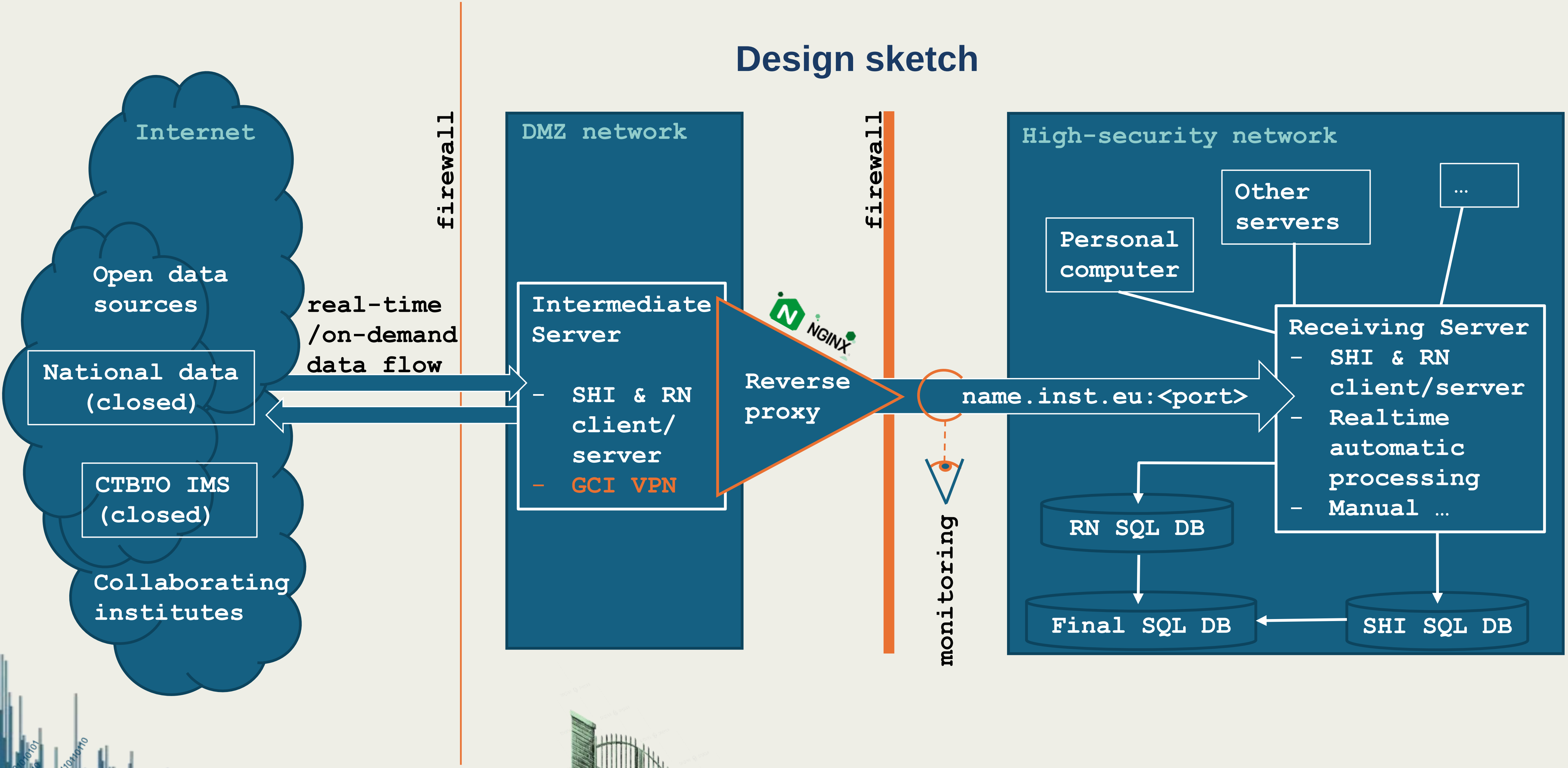


Secure Data Communication for Nuclear Monitoring at the Swedish NDC

Jon Grumer, Henrik Olsson, Marius Popa (CTBTO)

O4.2-647

Design sketch



FOI Swedish Defence Research Agency

Summary & Conclusion

- Modernization of waveform research at FOI required redesign of IT infrastructure
- Intermediate server located within e.g. a DMZ network
- Reverse proxy facilitates secure communication, also allowing data monitoring
- Deployment of IDC’s new VPN docker solution provides access to IMS in this system

→ A robust method for data communication

- At FOI, this setup now allows for direct access to data services that would otherwise only be reachable in a less secure network environment, as well as to the services within the GCI
- Allows for full functionality of e.g. SeisComP, in realtime, while simultaneously ensuring network integrity

- NDC’s - talk to IDC if you are interested in using the software VPN