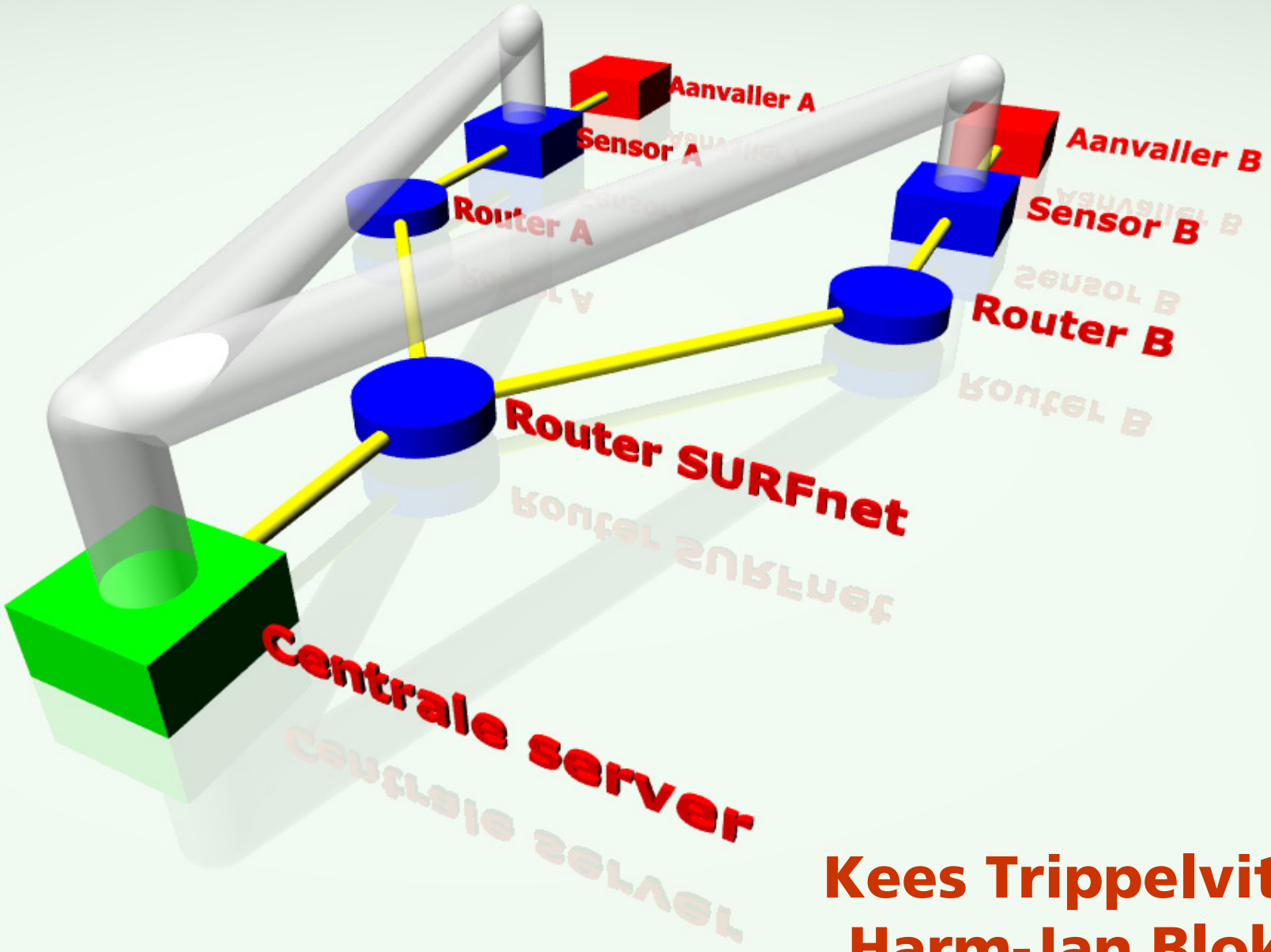
SURFnet IDS



Kees Trippelvitz
Harm-Jan Blok

Inleiding

- Doel van het project
- Gestelde eisen
- Projectinhoud
- Afbakening
- Onderzoeksmethode

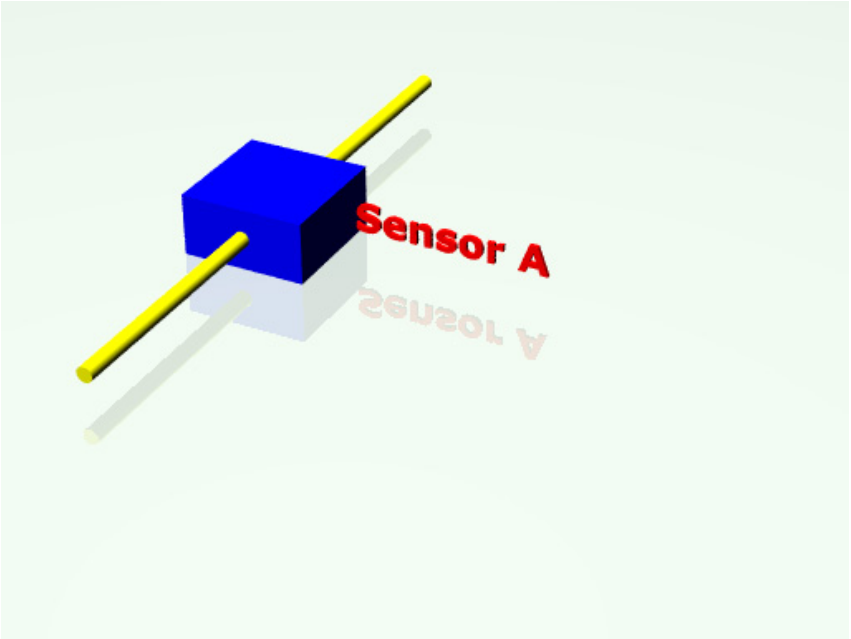
De sensor – Hardware

Eisen

- Plug en Play
- Onderhoudsvrij
- 1 of 2 netwerkkaarten

Mogelijkheden

- Hardware van instelling
- Thin-client
- Virtuele sensor



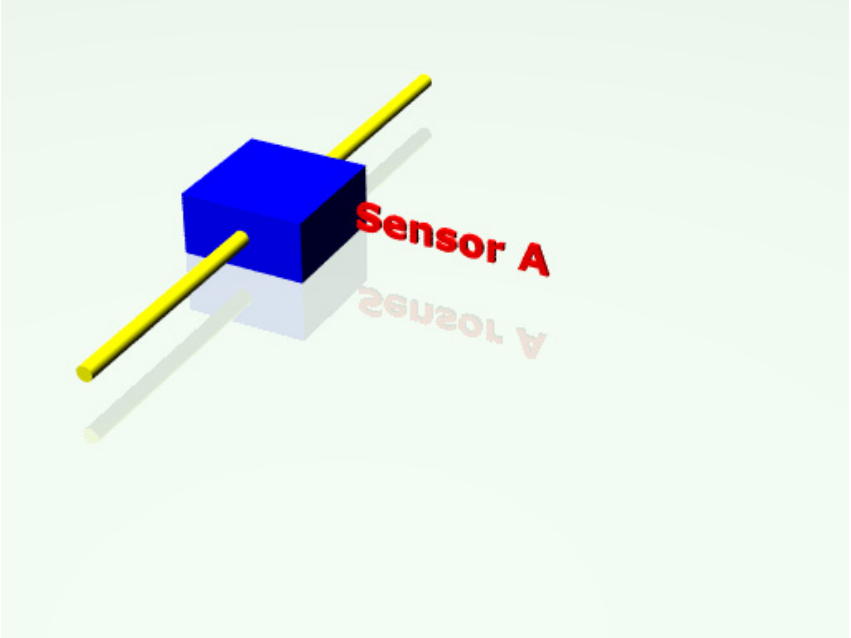
De sensor – Software

Eisen

- Onderhoudsvrij?

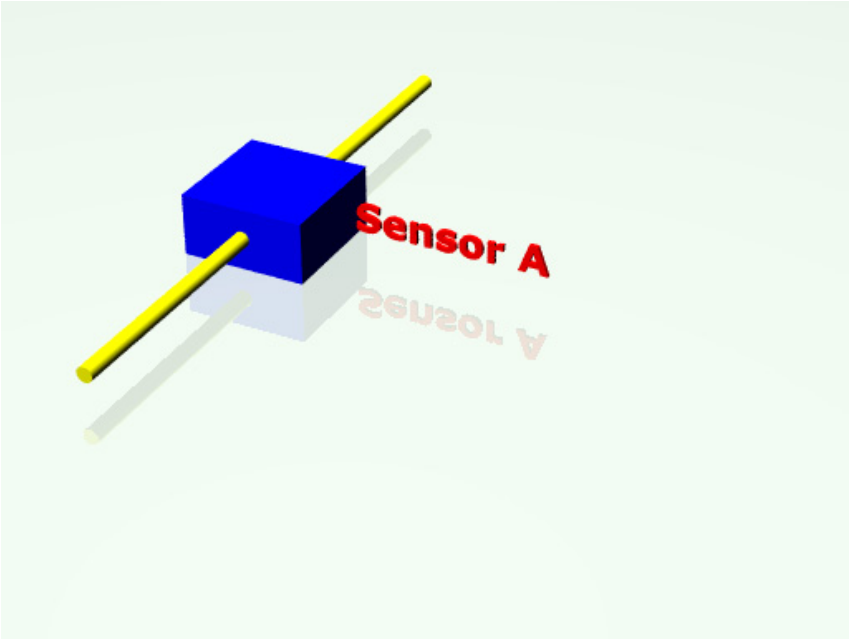
Mogelijkheden

- Live CD
- USB stick
- Netboot



De sensor – Proof of Concept

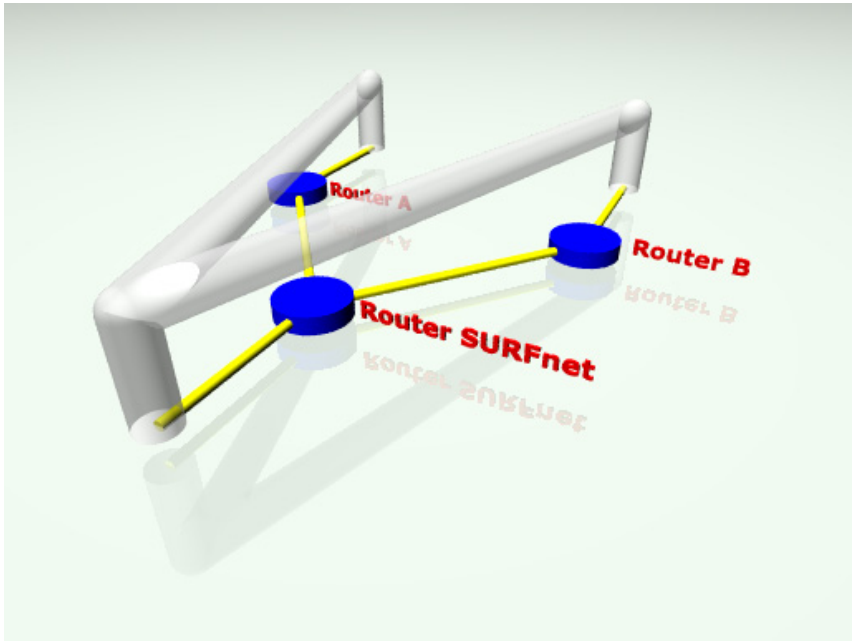
- Knoppix remaster
- Damn Small Linux
- Incrementeel



Wijziging strategie

- Pilot instelling TU Delft
- Interactie is gewenst
- Mogelijke oplossing
  - Sensor met honeypot
  - Centrale honeypot

Infrastructuur



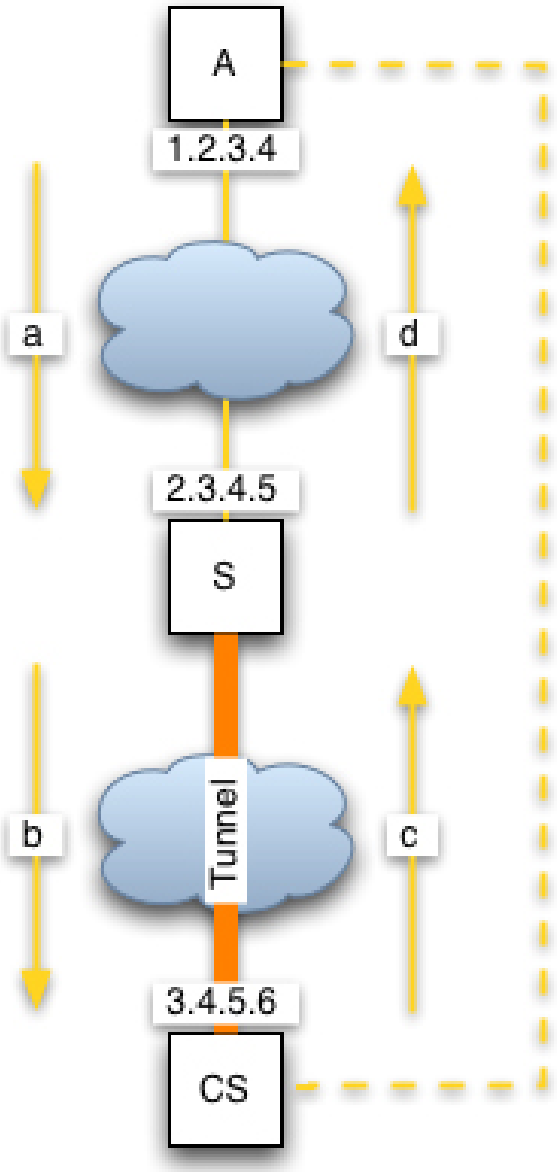
Eisen

- Plug en play
- Onderhoudsvrij
- Veilig/encryptie
- Laag 2 verkeer versturen

Oplossing

- OpenVPN

Proof-of-concept

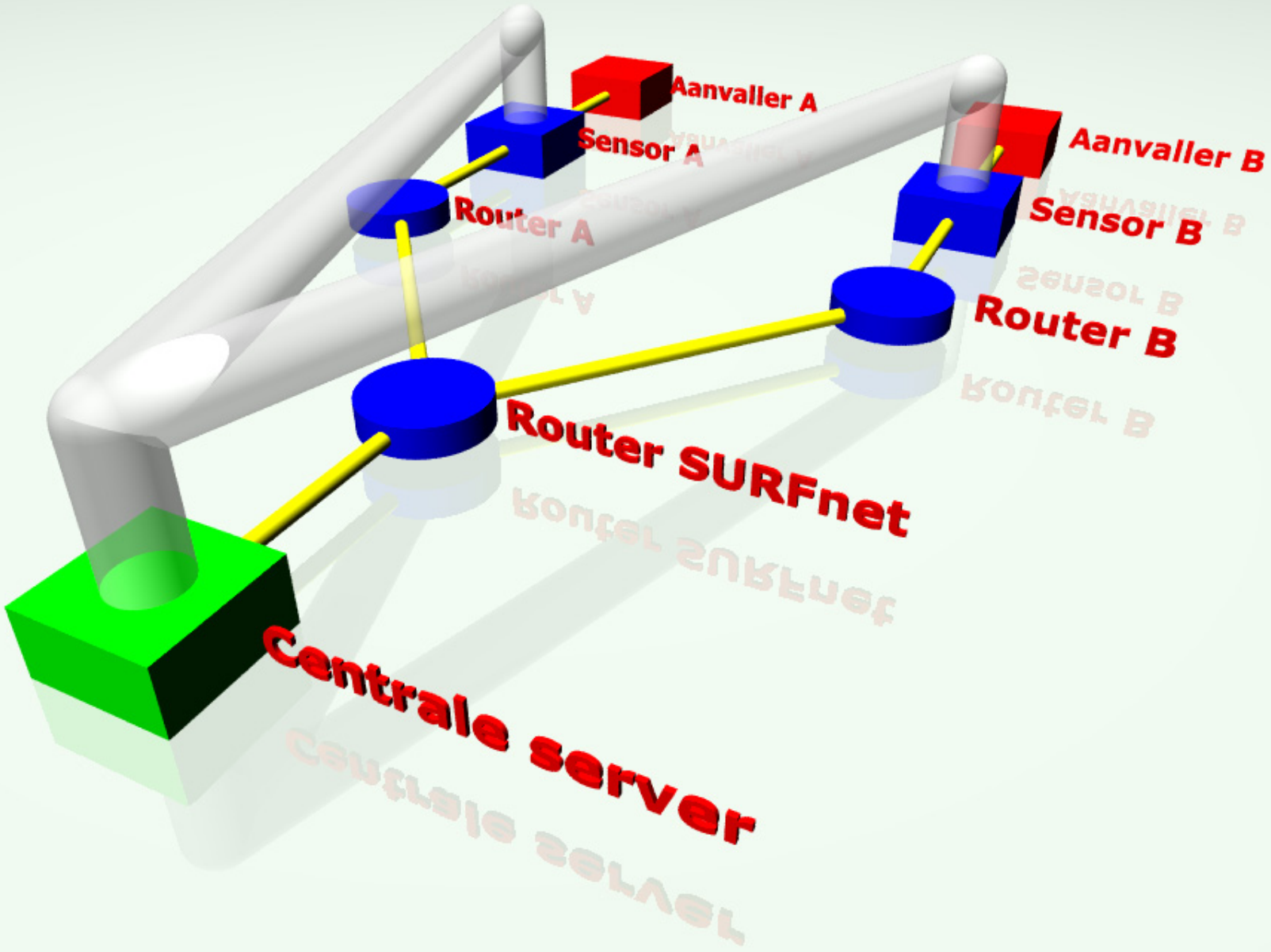


Problemen

2. Afzenderadres
3. Routering terug
4. Andere bestemming

Oplossing

7. NAT
8. Virtuele interface


Aanvaller A
Sensor A
Router A
Aanvaller B
Sensor B
Router B
Router SURFnet
Centrale server

Conclusie

Hardware

- Beschikbare hardware

Software

- USB stick
- Linux, ‘eigen’ distributie

OpenVPN

Honeyd centraal (honeypot)

Vervolg onderzoek

- Sensor volledig plug en play
  - Certificaten
  - Updates (DNS, HTTP)
  - Detectie IP adres doorgeven
- Centrale analyse

http://www.os3.nl/~hjblok/