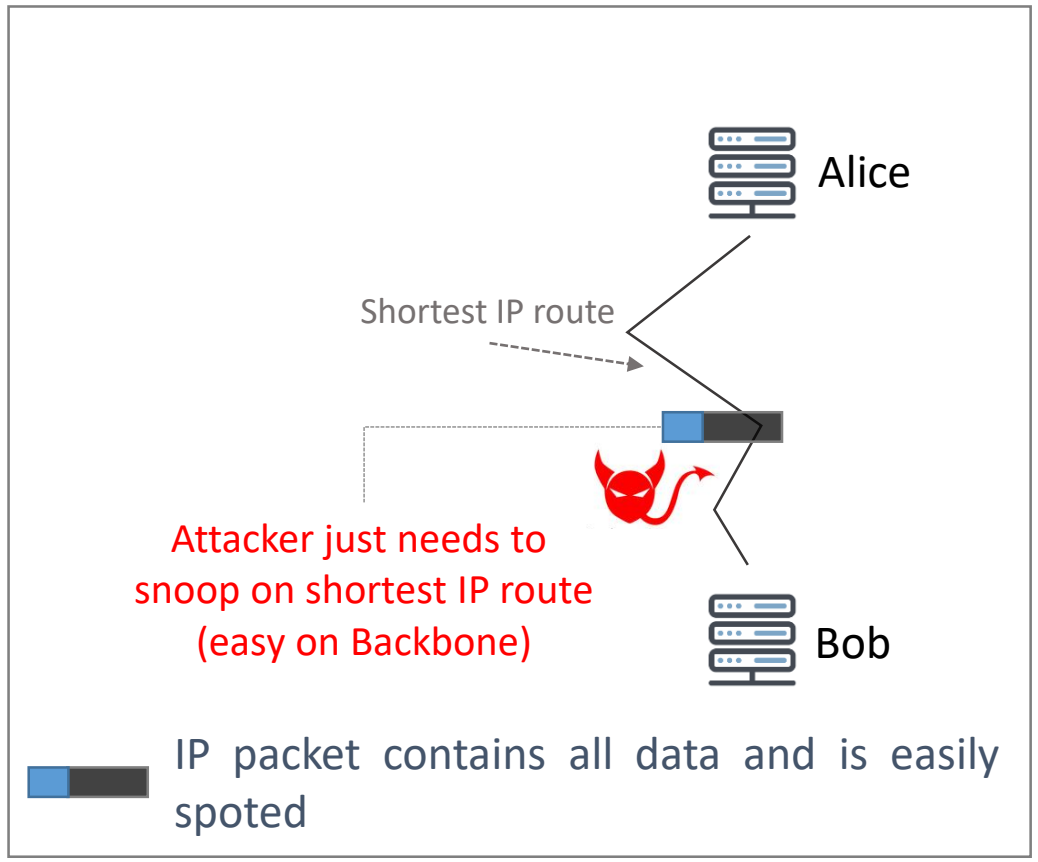
Snowpack

Building the Beyond-Trust Internet

Baptiste Polvé, Research Engineer, CEA List &
Snowpack's future CTO

New Paradigm for Network Security & Privacy (1/2)

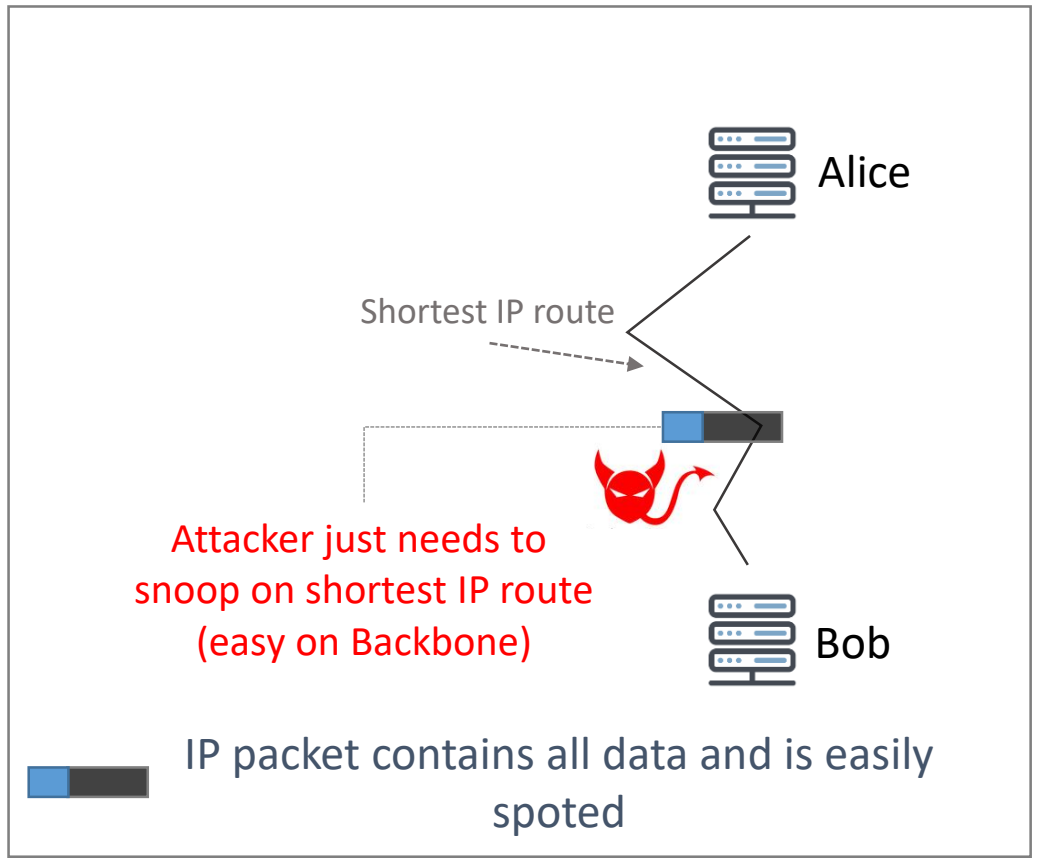
Security today: relying mainly on crypto



- **Mass decryption is complex but there is a possibility to identify communication metadata used for routing**
  - Access to identities or at least large company VPN provider
  - Targeted attacks (side-channel)
- **Robust cryptographic system but vulnerable**
  - Implementation
  - Maths vs Computing power
  - Trusted Third-Party
- **Seems to be related to the fact that privacy is opposed to security**

New Paradigm for Network Security & Privacy (2/2)

Security today: relying mainly on crypto

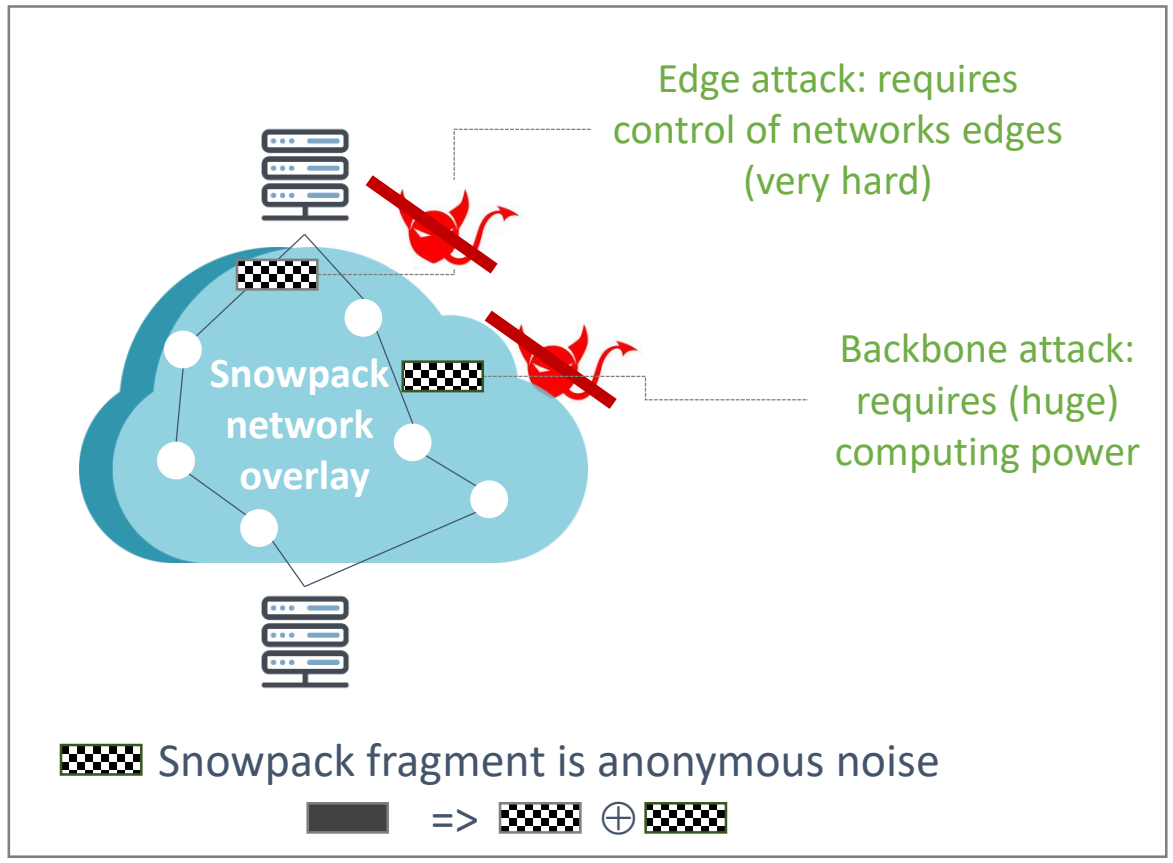


Edge

Backbone

Edge

Snowpack: relying on noise and multiple routes



Snowpack properties

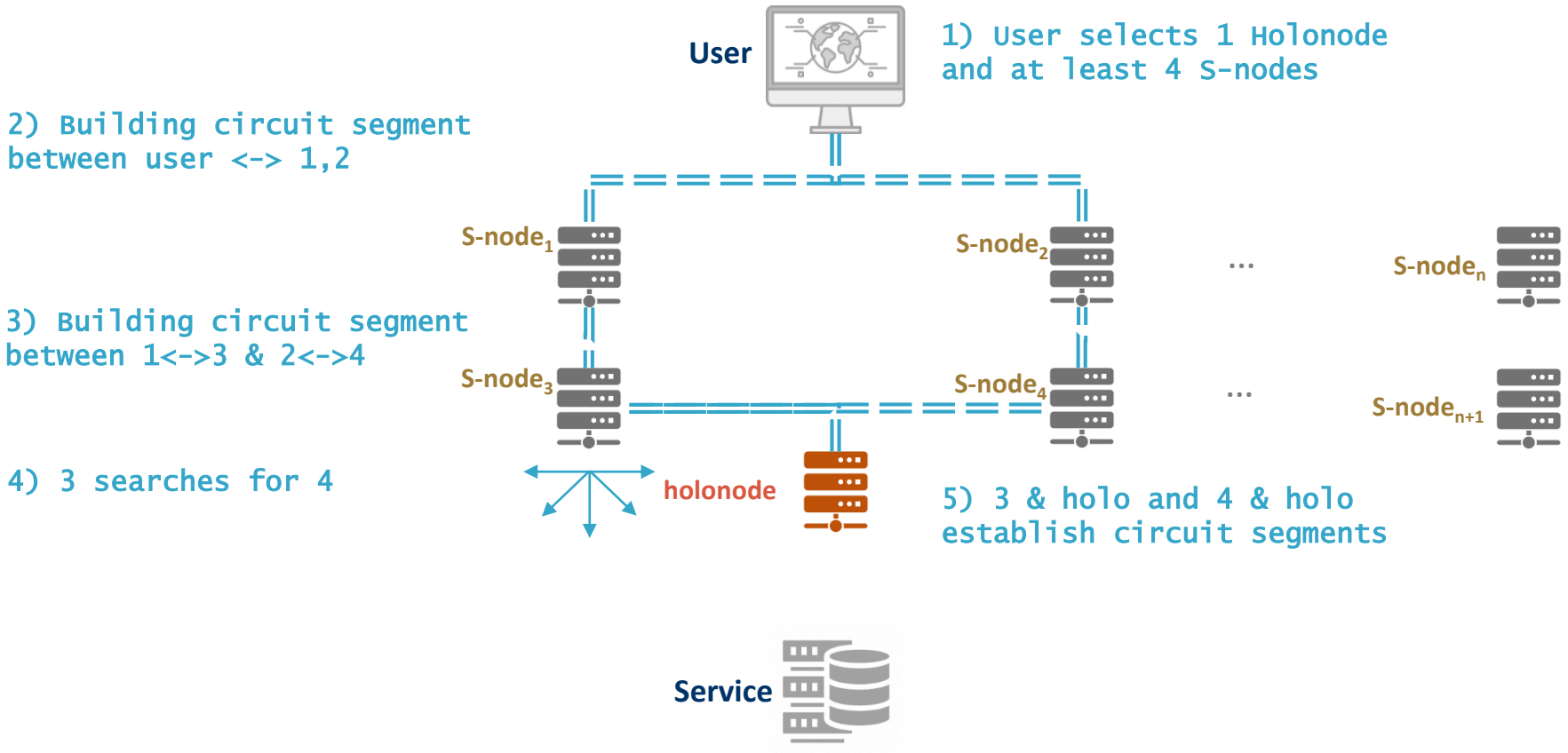
Principle

None of the materials used for the communication should have access to all the key elements of a communication: {Sender, Recipient, Content}

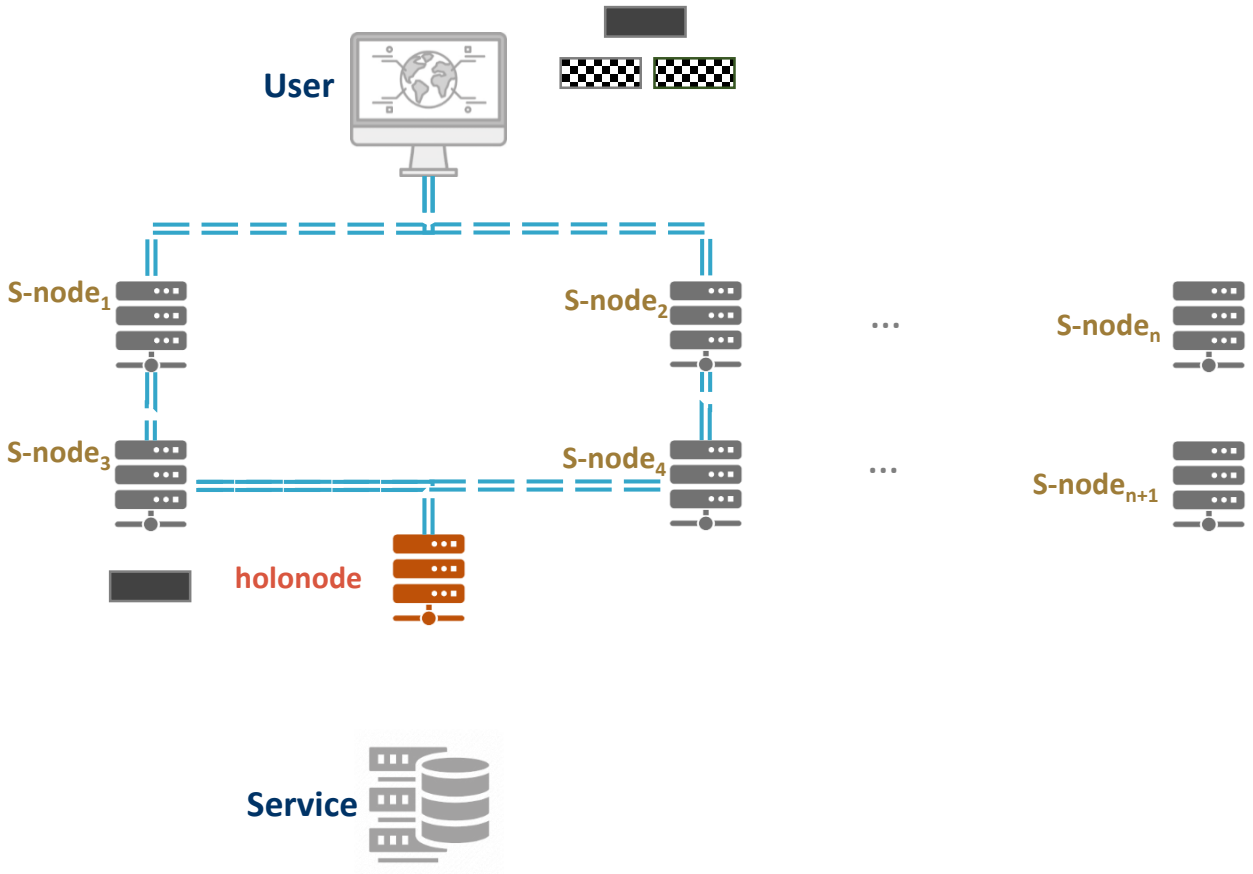
Privacy Mode

Security Mode

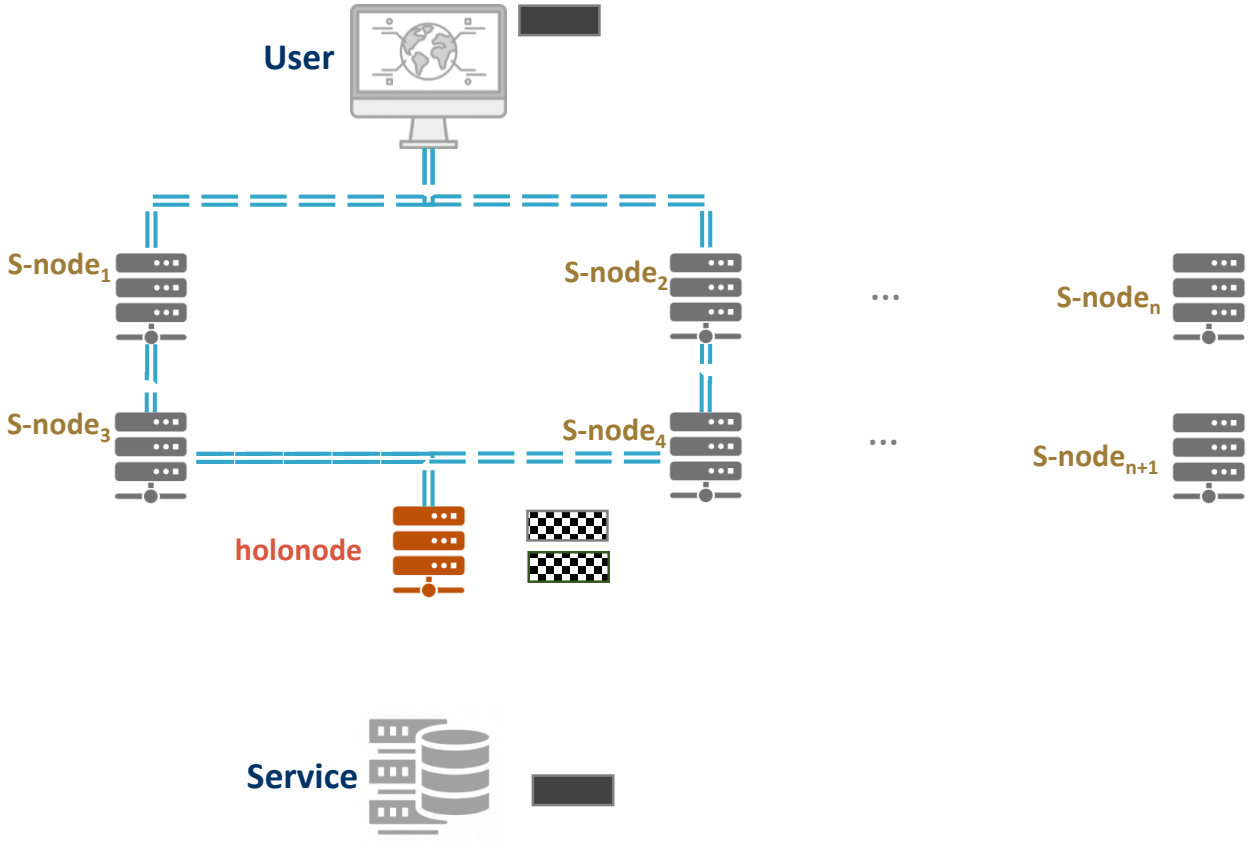
Snowpack main protocol principles – Privacy Usage
Step 1: building route



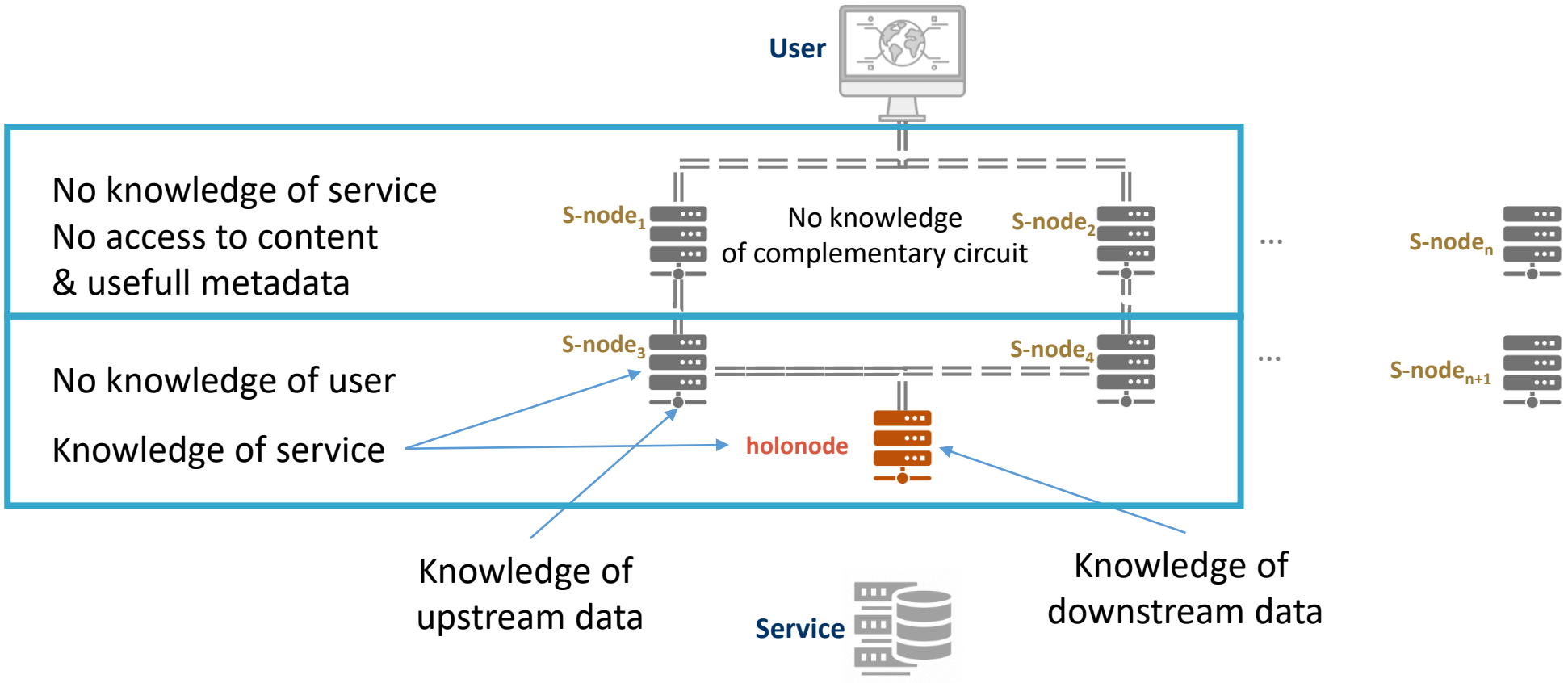
Snowpack main protocol principles – Privacy Usage
Step 2: sending packets



Snowpack main protocol principles – Privacy Usage
Step 3: receiving packets



Snowpack main protocol principles – Privacy Usage
Summary of privacy properties

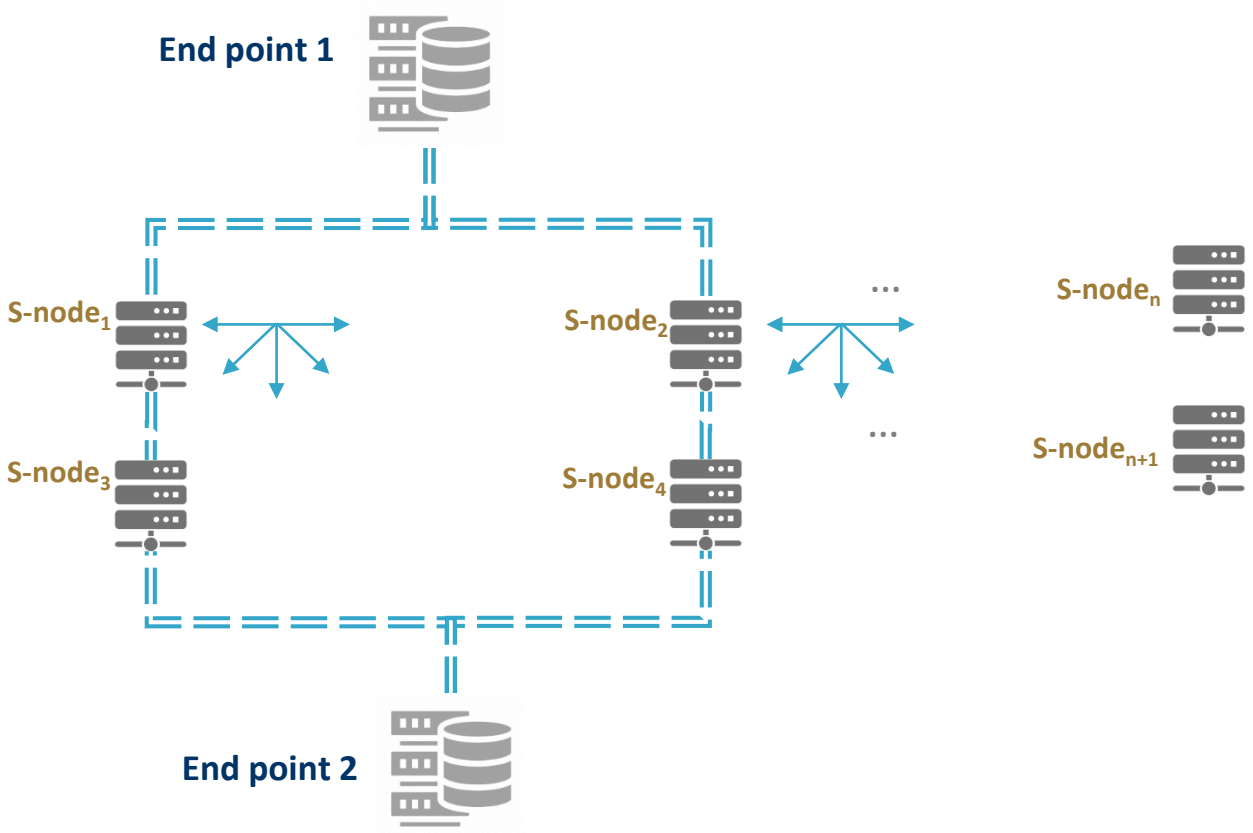


Snowpack main protocol principles - Security usage

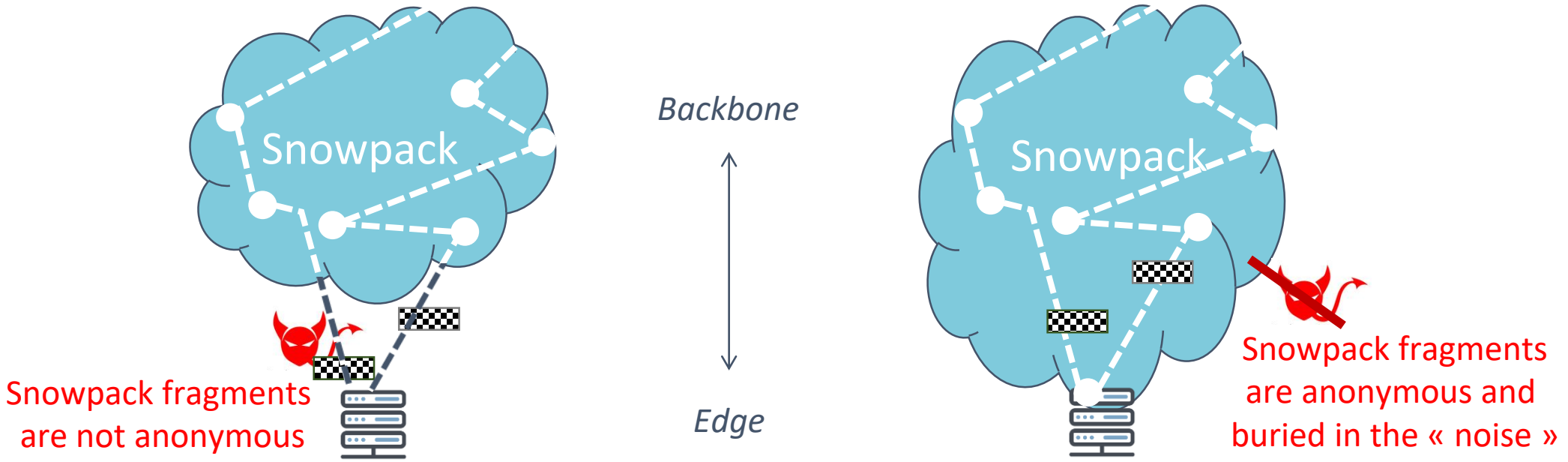
1) Building circuit segments between EP1<->1,2 & EP2<->3,4

2) 1 & 2 search for 3 & 4

3) Connexions 1<->3 & 2<->4



Users may become elements of Snowpack's infrastructure to increase their privacy



Snowpack properties

Principle

None of the materials used for the communication should have access to all the key elements of a communication: {Sender, Recipient, Content}

Privacy:

Much harder attack through traffic analysis

No potentially vulnerable trusted-third party

Possibility to hide communication from Edge

Security:

3 encryption levels

No MITM

Obfuscated attack surface

Network Security outpost

Additional features from central & distributed supervision:

Capacity to guarantee Privacy & Security levels

Capacity for users to modulate these levels

Capacity to challenge nodes code from central & user level

Demonstration

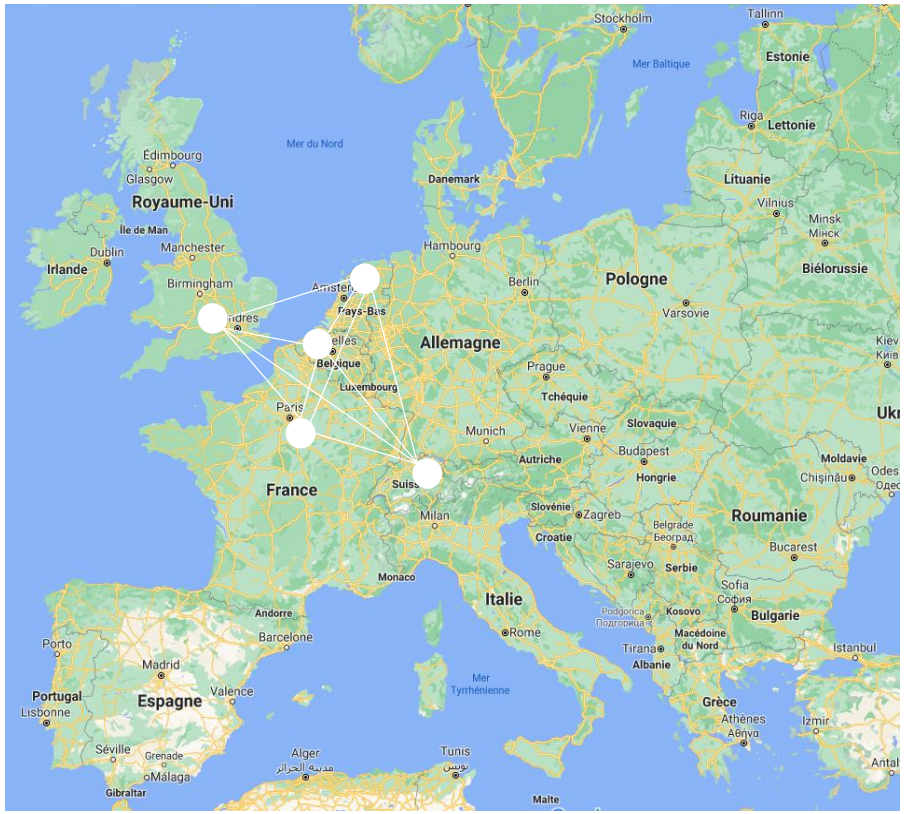
DEMO

Where do we stand

- **Deployed in lab on different local clouds**
  - Privacy mode integrated
  - Each node can connect with up to 256 clients or nodes
  - Multi-user browsing simultaneously
  - Quasi seamless performance for standard browsing

- **Ongoing deployment on +50 nodes across Europe as a beta version for Privacy use-cases**

- **Next:**
  - Security mode
  - Other cloud environment
  - Complete seamless performances
  - 2 years R&D roadmap with additional properties



Thank you !

Contact: baptiste.polve@cea.fr or via linkedin.