

Snowpack

Become Invisible



Agenda

- Quick intro on Snowpack
- The technology
- Testing & Deploying



Quick intro



Snowpack Founders & Management Team

Frédéric LAURENT
CEO

Aerospace Engineer (ISAE)
Master in ICT Management (EM Lyon)
HEC Challenge+ 2020
15 y. in European ICT & Security lobbying & prog. mngt.
Lead author of Snowpack patents



Sébastien GROYER
COO

Engineer & PhD
Almost 20 years as VC (CDC-E – Masseran – Seventure)
Start-up financing, growth and management
(50 startups)



Baptiste POLVÉ
Technology & Developments

Telecom Engineer (Telecom SudParis)
HEC Challenge+ 2020
3 y. in cybersecurity research in CEA
ANSSI certified



David Gonzalez
Sales & Partnerships

Master from Bordeaux Management School
20 years in telecom industry (Telstra, Tata, Colt, Orange) incl. 14 y. as French/ Intl Sales Director

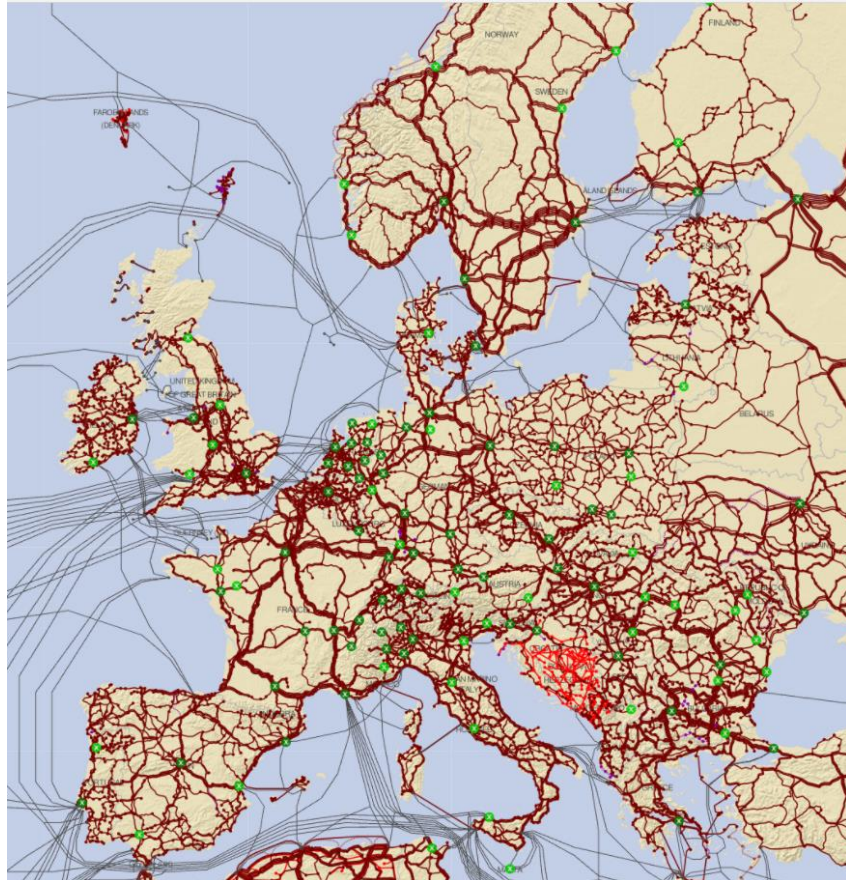


Spin-off created in May 2021 (CEA-Investissement is a co-founder), based in Orsay (91), France

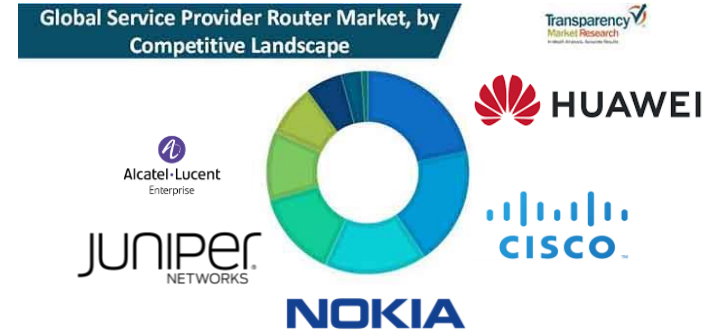


State of play / Environment

- 70-80% of Internet traffic to US & subject to Cloud Act
- US & China main vendors of Core Service Provider routers



Global Service Provider Router Market, by Competitive Landscape

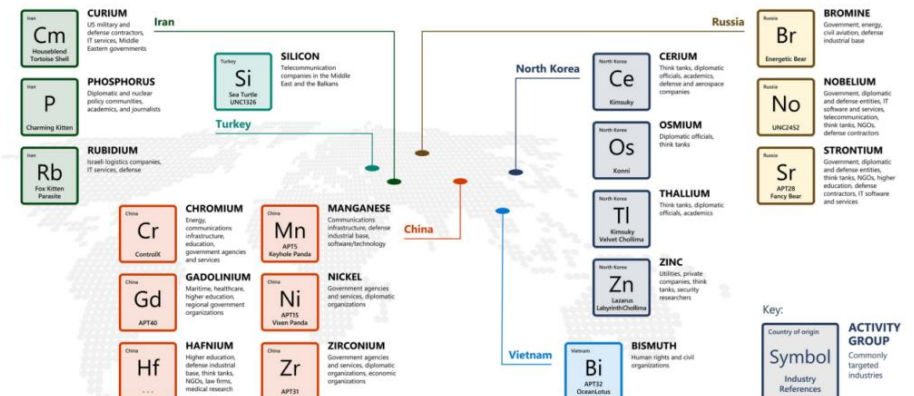


- Main vendors of Deep Packet Inspection / Lawful interception



- State-sponsors APT (continuum hackers – States)

Sample of nation state actors and their activities



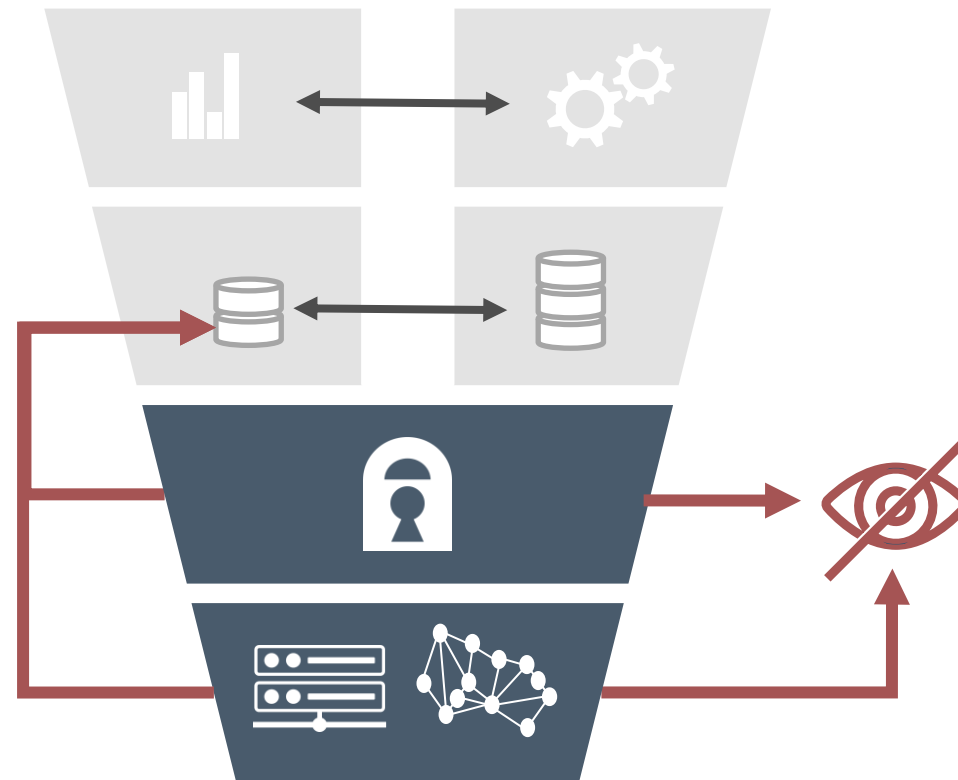


Snowpack makes you invisible to network attacks

Trust-based, Visible Systems



Each element is a potential breach



Invisible, Secured by Snowpack



Hackers can't see data

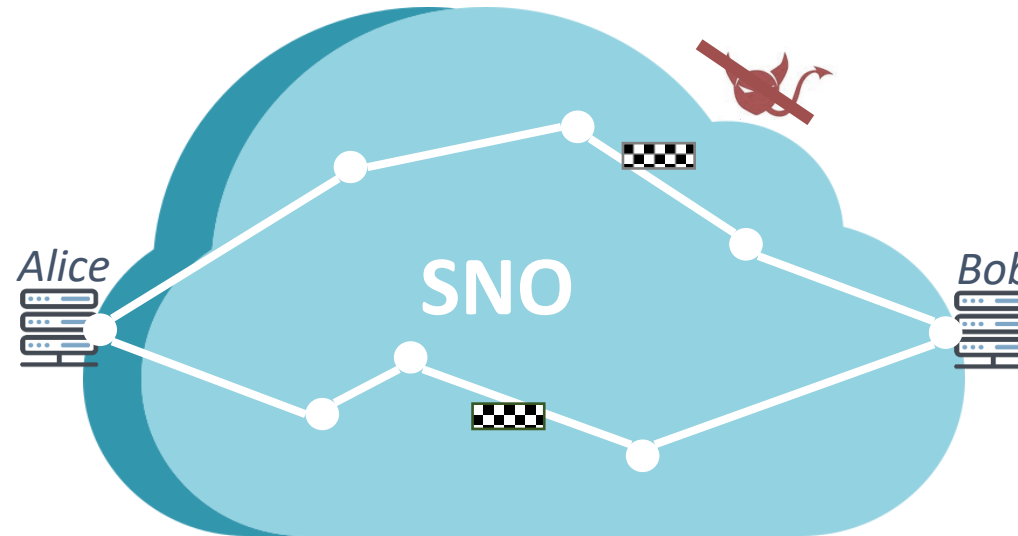


The Snowpack Network Overlay (SNO) makes you invisible (even to us)



3 patents
2017 2019 2021

No specific HW & SW requirements



Impossible to track & hack
 ↓
 No need to trust infrastructure

 Snowflakes move through SNO, Snowpack Network Overlay

A single international network overlay made of:

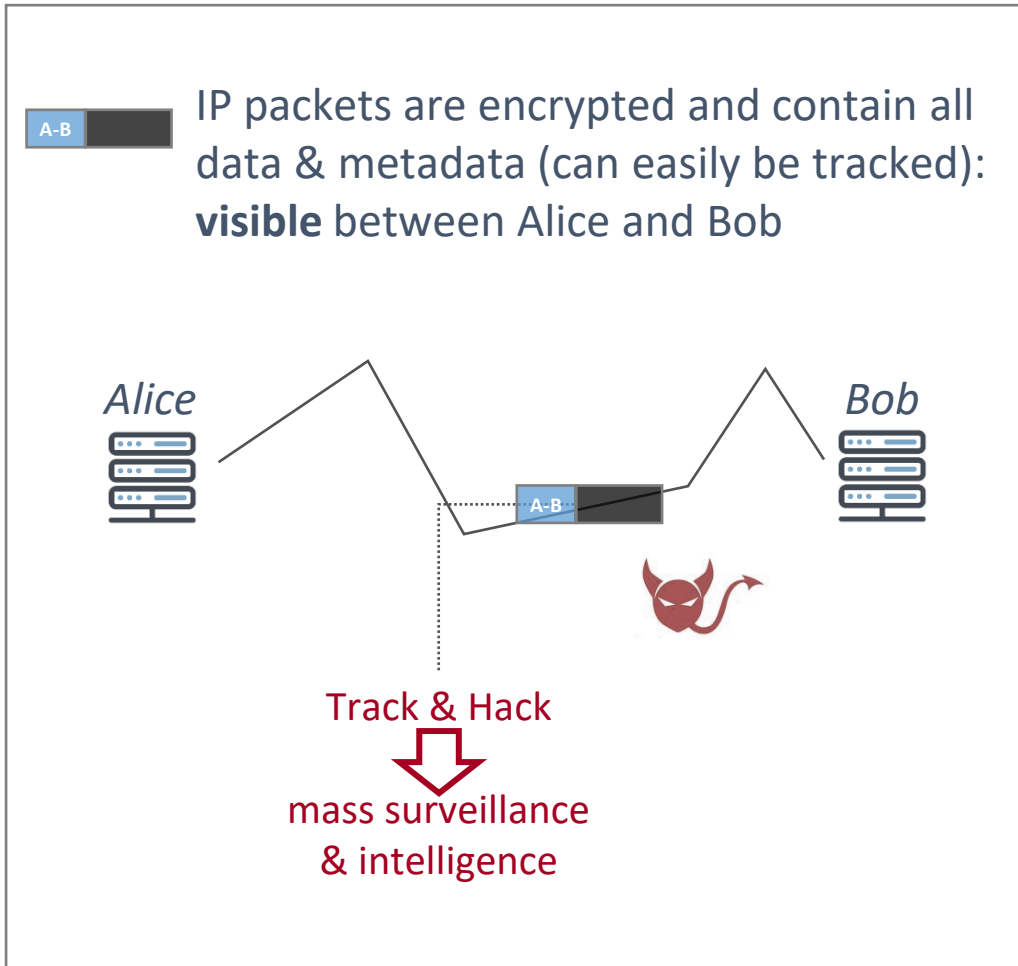
- **software** running on servers operated by clients, Snowpack and other third parties (heterogeneity)
- connectors turning IP packets into 'snowflakes' (i.e. anonymous random bytes / noise)

Breaking Snowpack system requires collecting all snowflakes and identifying complementary snowflakes: almost impossible with enough data and traffic

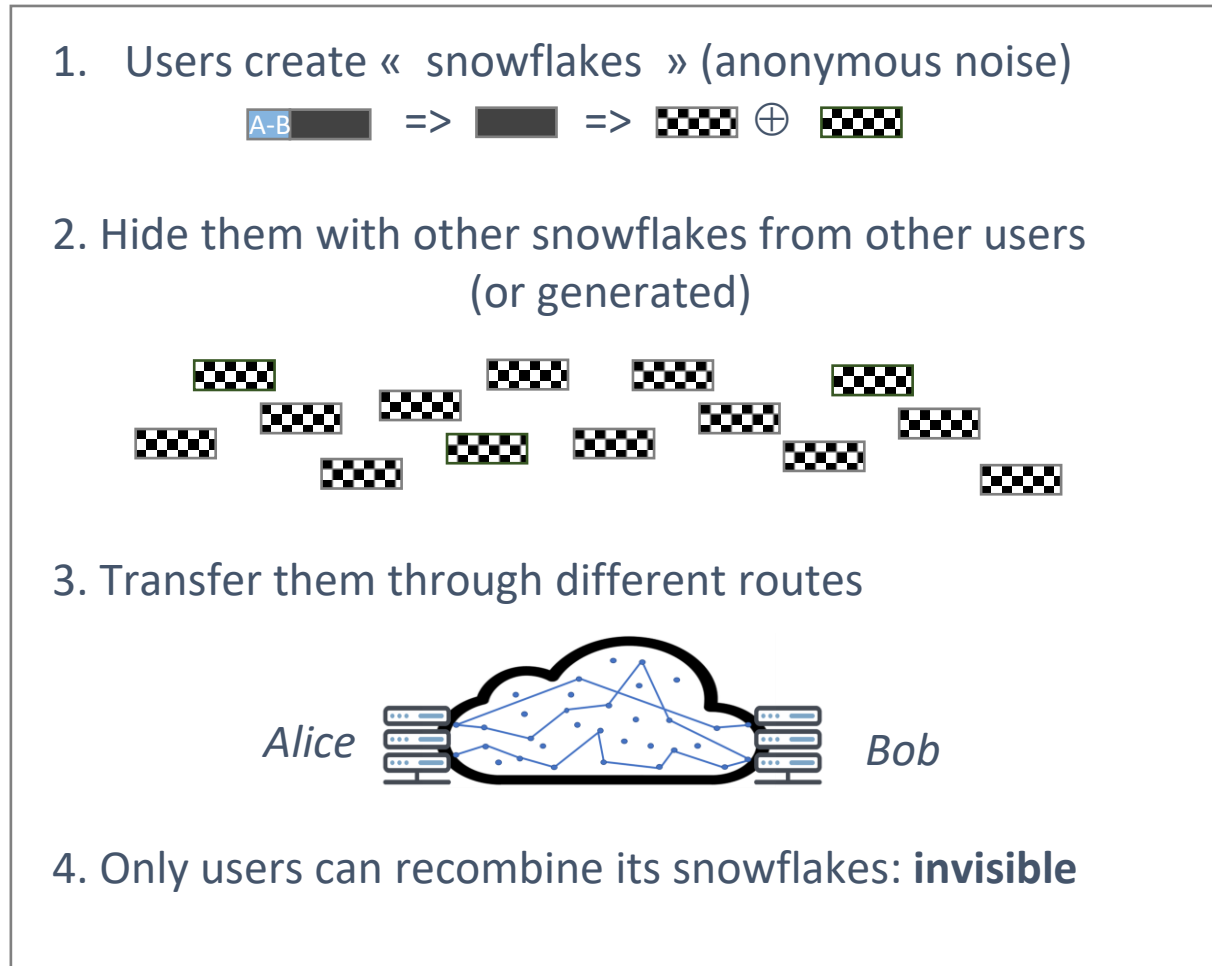


Snowpack: network anonymity & security combined in one product

Security today: crypto only



With Snowpack: best anonymity and security





Snowpack, the Invisibility Overlay Network



Invisible presence on Internet
Users, servers, data/communications



Resilience
Resistance against kill-switch/DoS



Protection against surveillance
From Hackers, ISPs and States



Forward secrecy
Future proof resistance against quantum computer-based attacks



Hidden attack surface
Entry and exit servers are stealthy



Customized solution
Several tailored offers to fit your needs



Snowpack: Competition

Privacy & Security

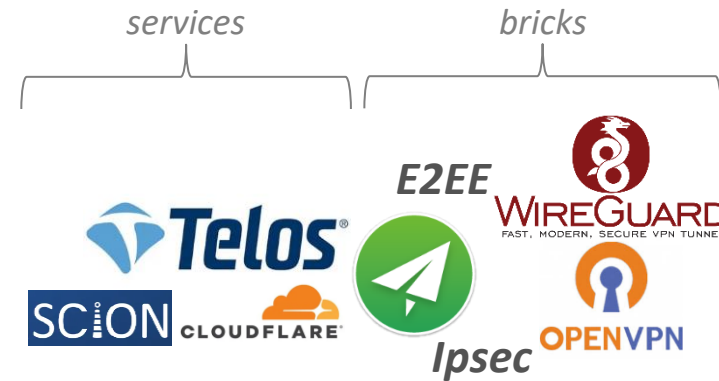
Beyond-trust technology

Quantum Communications

Snowpack



"trusted" third party with crypto



Use-case specific

Many use-cases

General-purpose

Use of Technology



The technology



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

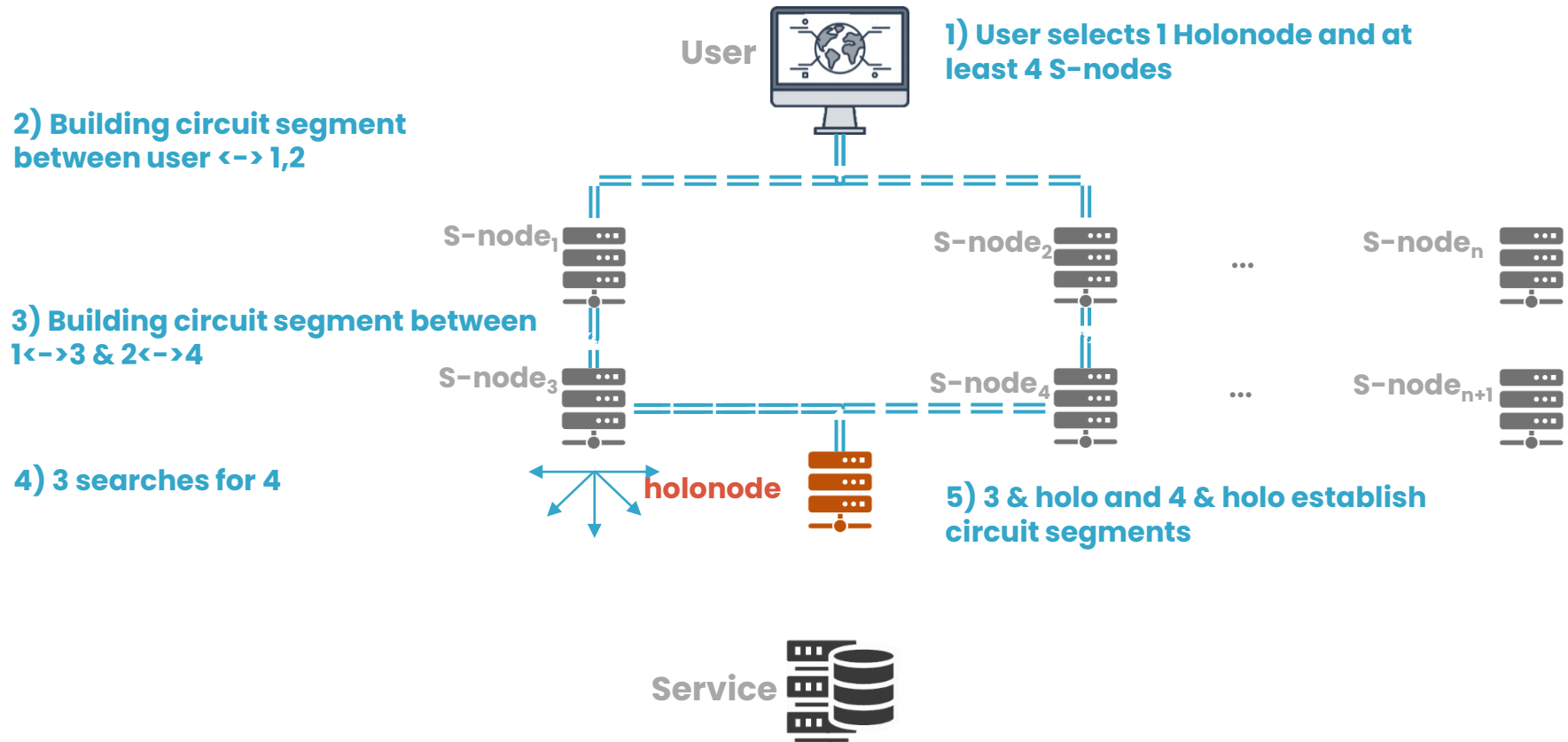


Security Mode



Snowpack main protocol principles – Privacy Usage

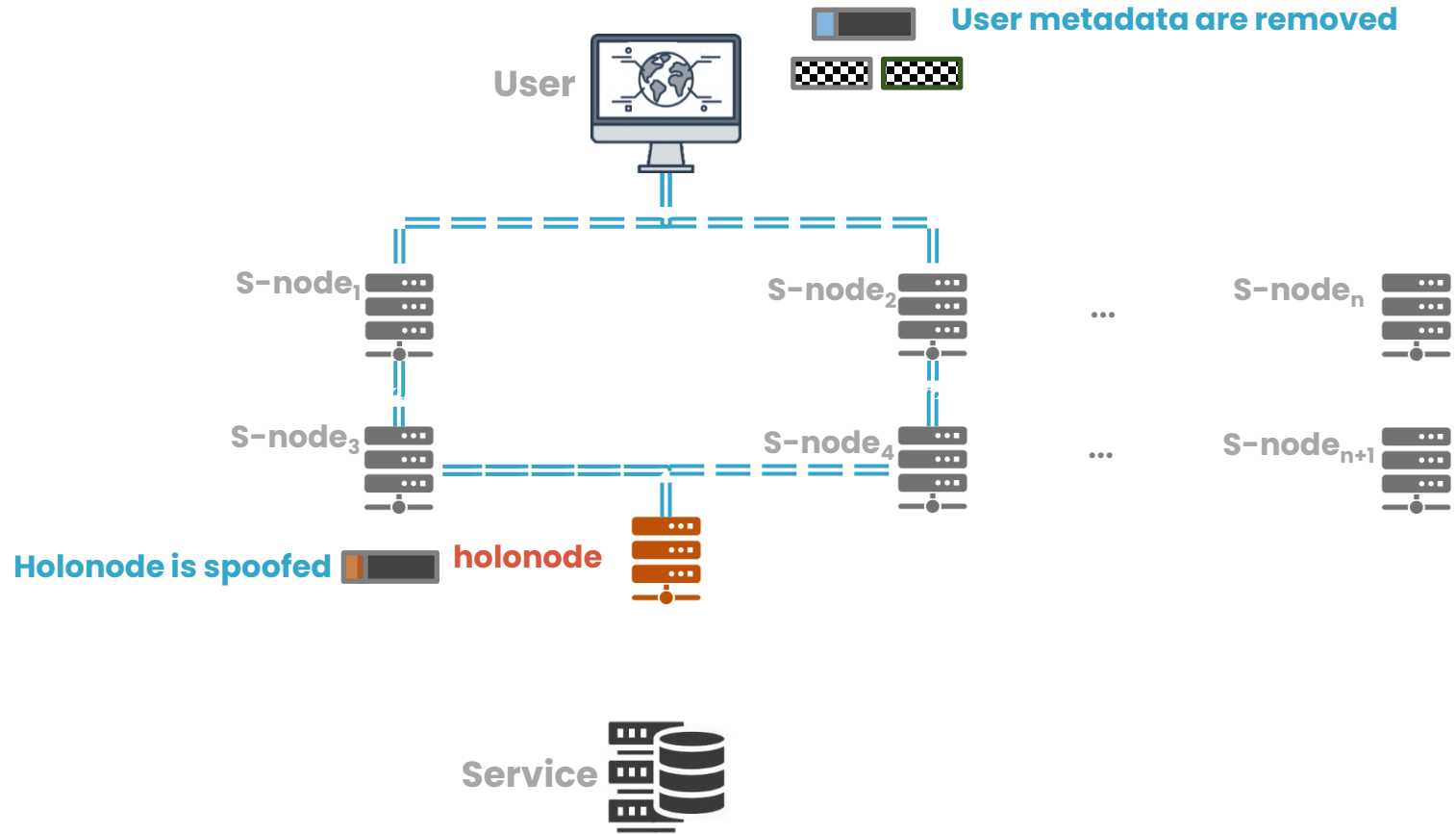
Step 1: building route





Snowpack main protocol principles – Privacy Usage

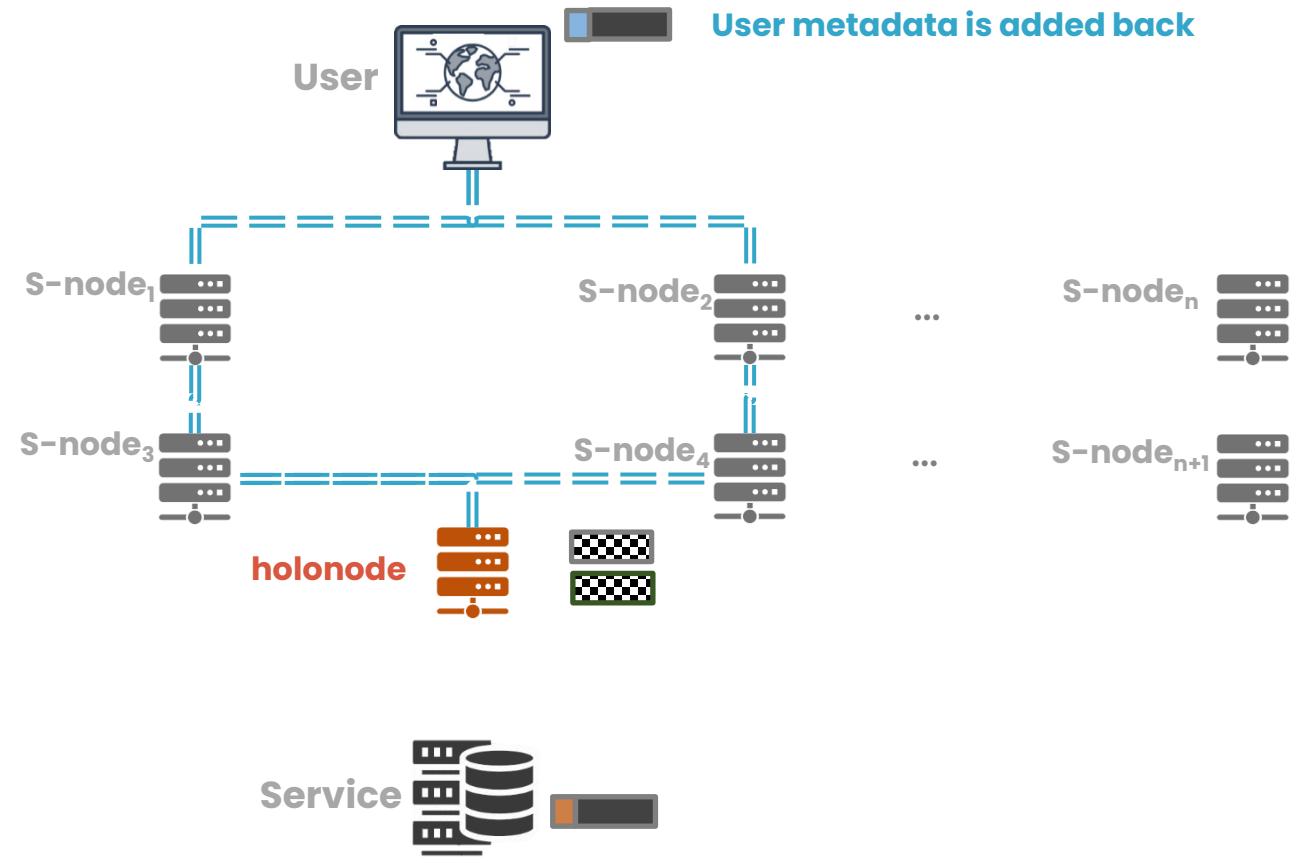
Step 2: sending packets





Snowpack main protocol principles – Privacy Usage

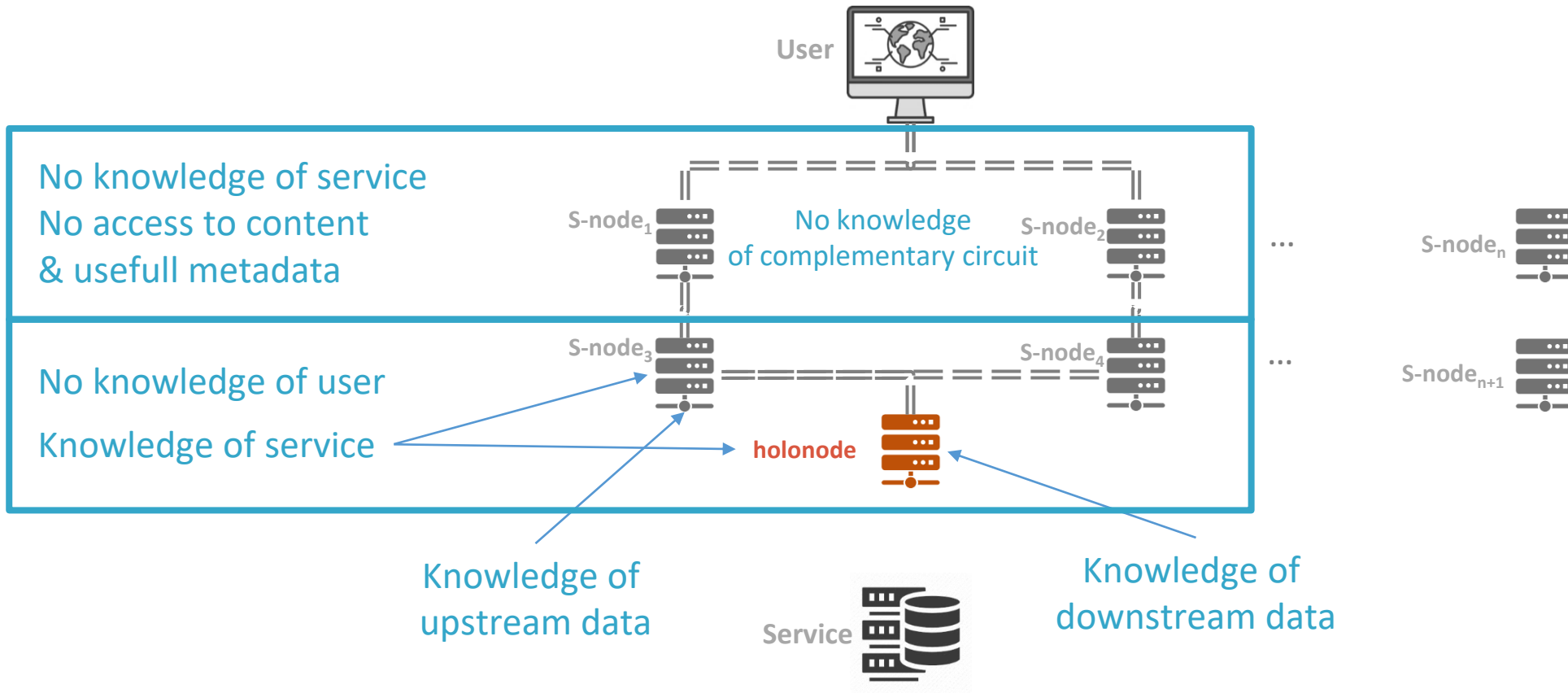
Step 3: receiving packets





Snowpack main protocol principles – Privacy Usage

Summary of privacy properties





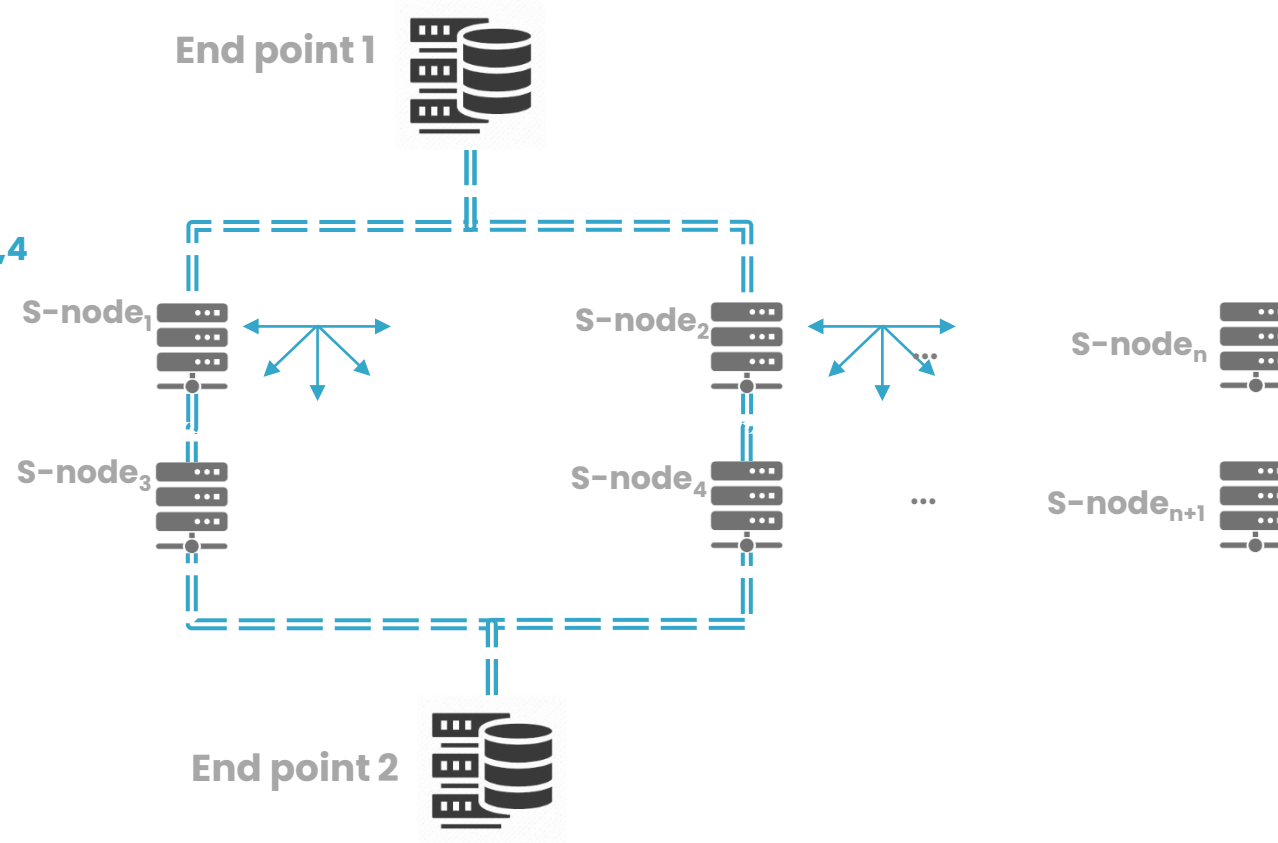
Snowpack main protocol principles - Security usage

Step 1: building route

1) Building circuit segments between EP1 \leftrightarrow 1,2 & EP2 \leftrightarrow 3,4

2) 1 & 2 search for 3 & 4

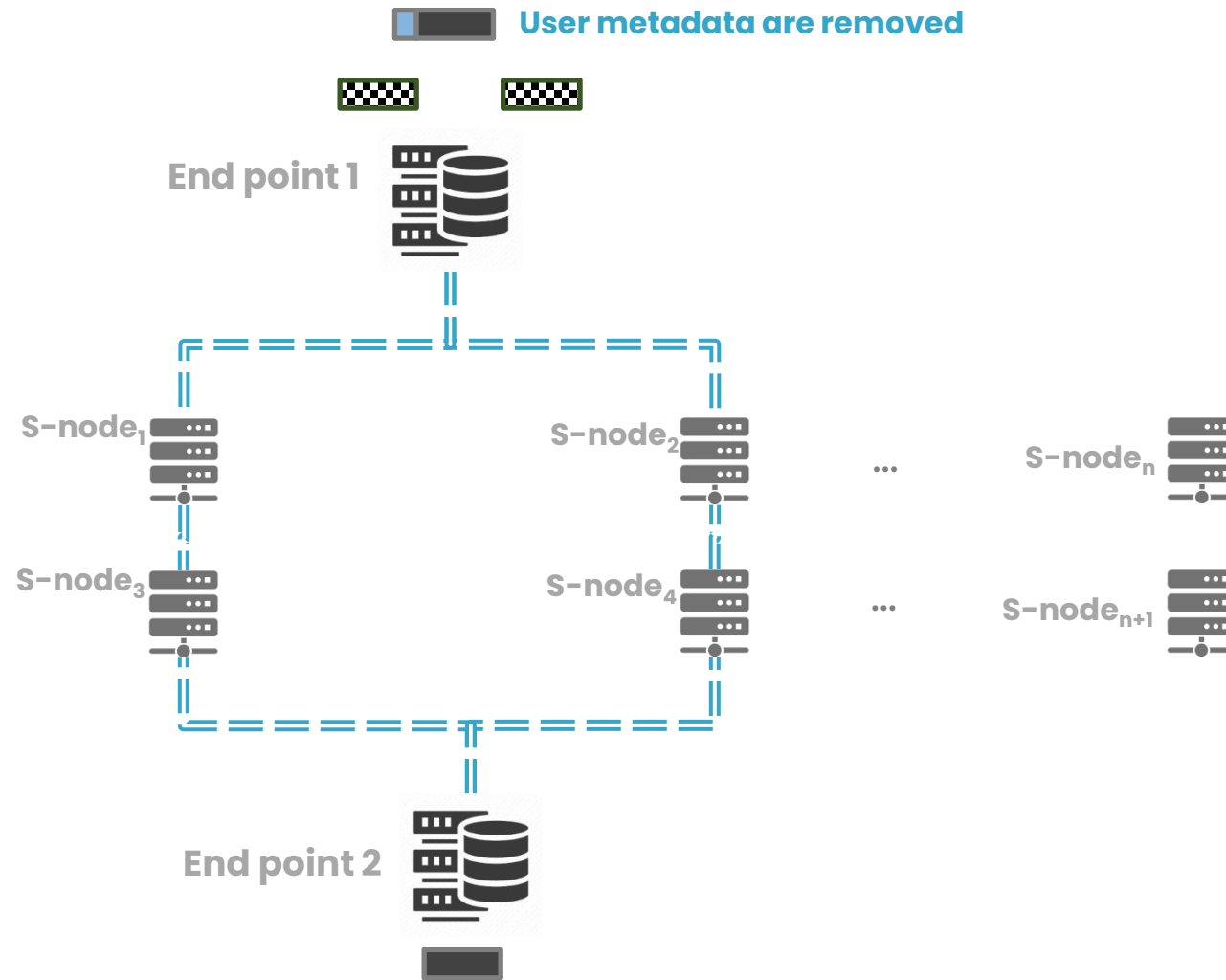
3) Connexions 1 \leftrightarrow 3 & 2 \leftrightarrow 4





Snowpack main protocol principles - Security usage

Step 2: Communication





Snowpack properties

Principle

No element 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:

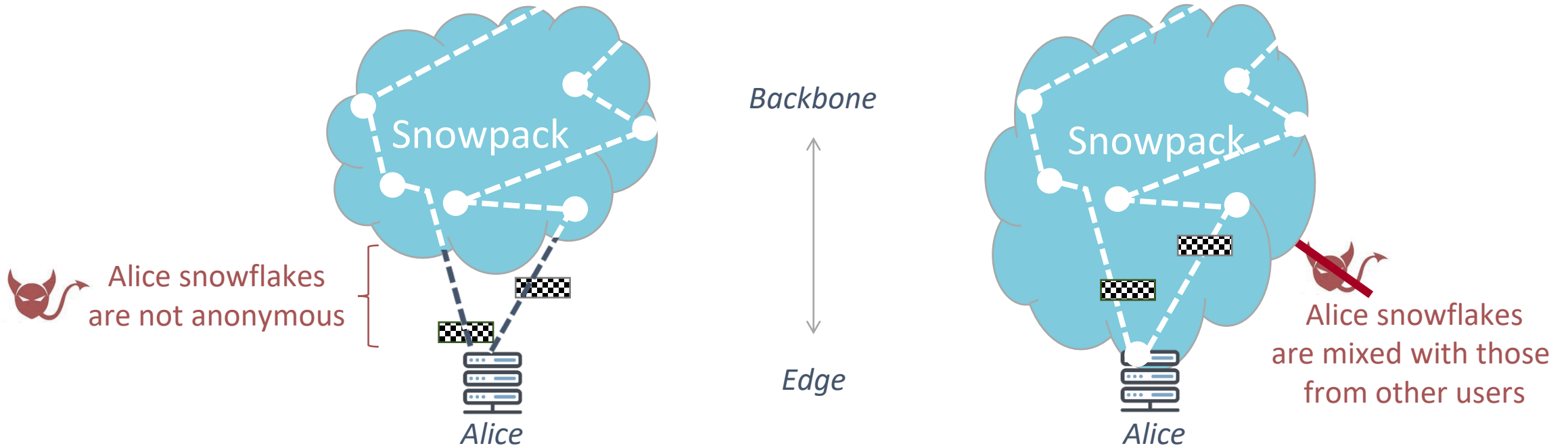
3 encryption levels
No MITM
Obfuscated attack surface
Network Security outpost

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



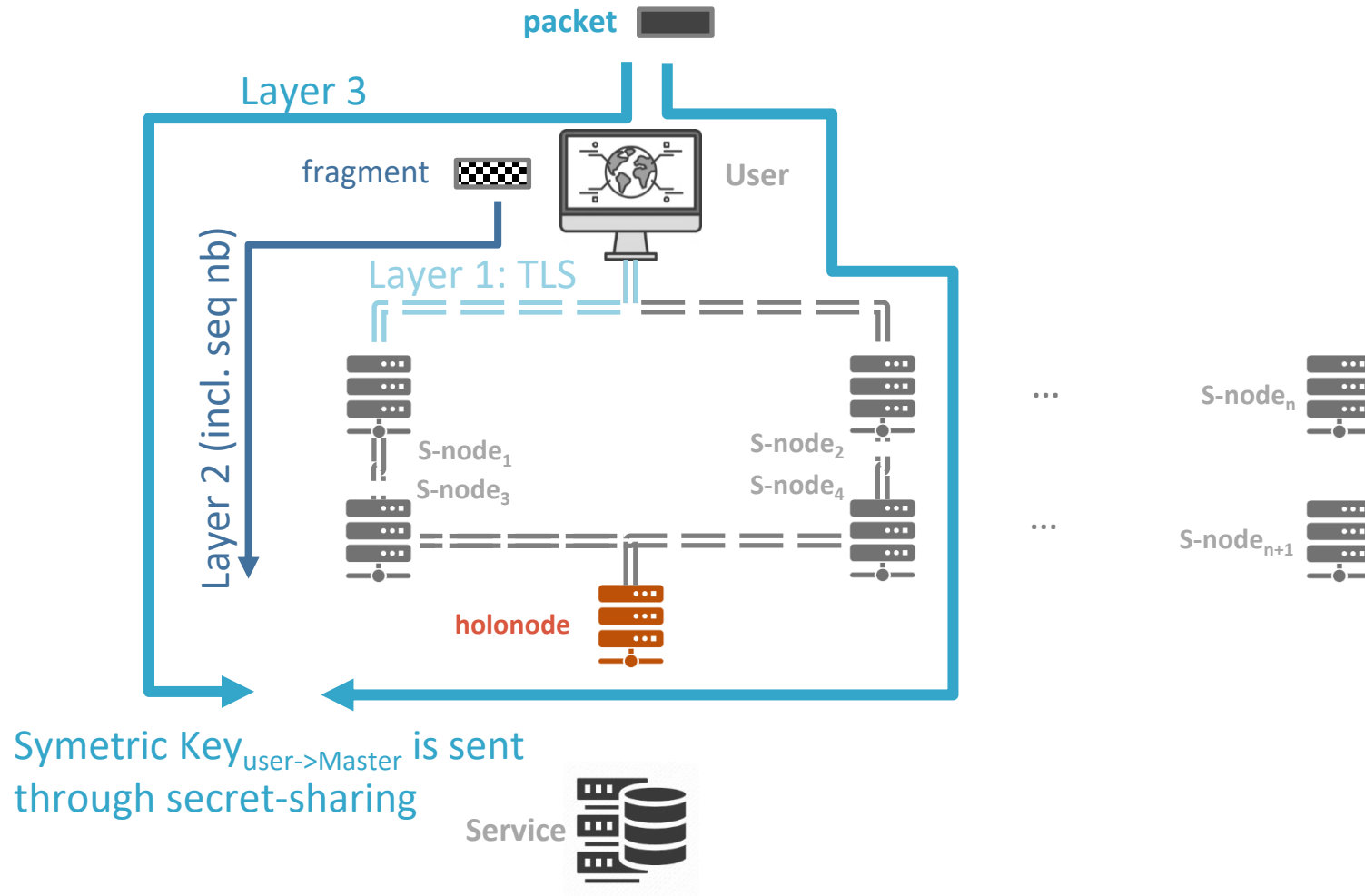
Becoming part of Snowpack's infrastructure increases invisibility





Crypto layers (Privacy mode)


PKI
Used for:
Layer 1
Layer 2



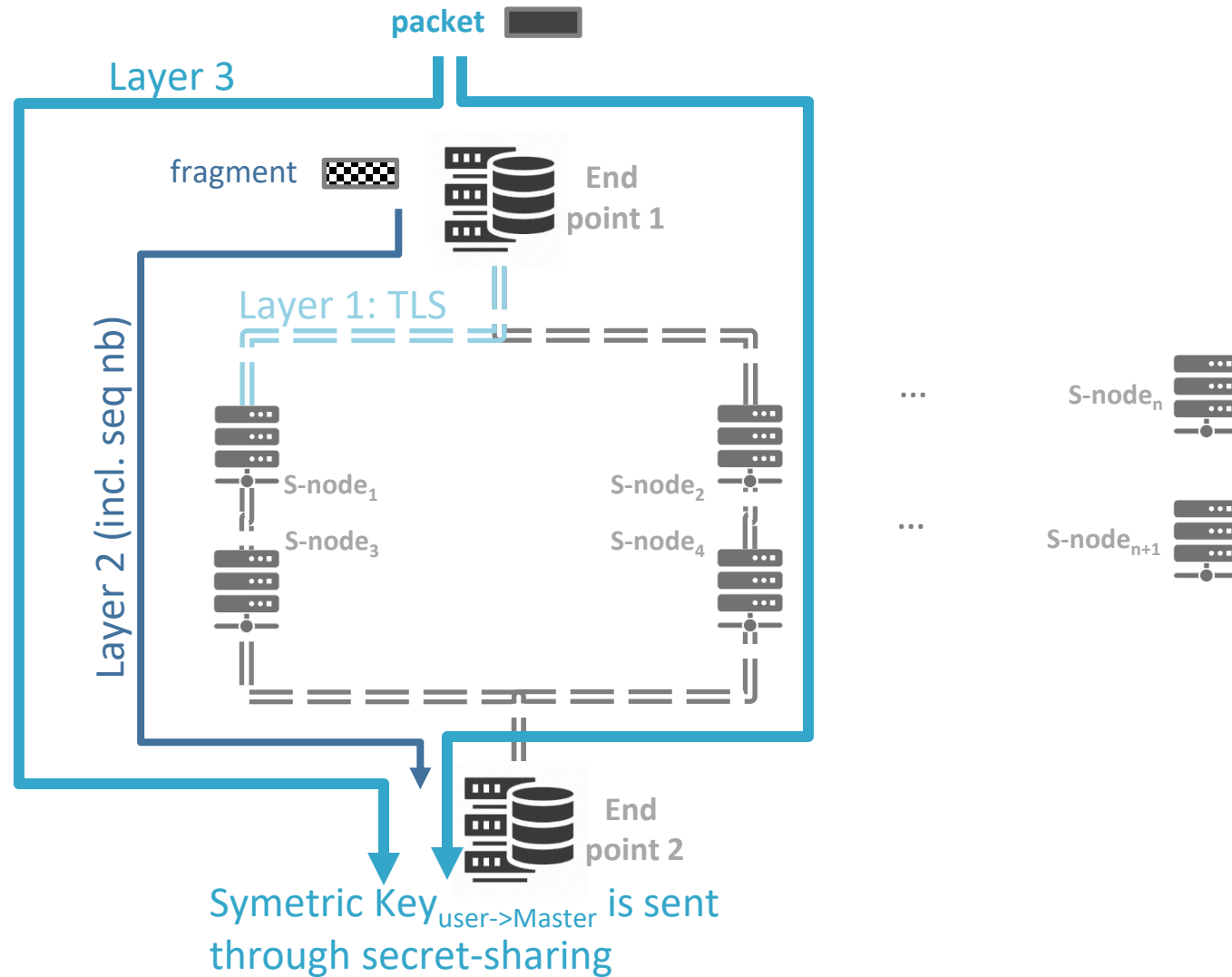


Crypto layers (Security mode)



PKI

Used for:
Layer 1
Layer 2





Snowpack resistance if all encryption is broken

Value description	Value notation
Number of fragments issued from one packet	F
Number of packets currently transiting via snowpack	N

For TOR or VPN technologies, it is instant.

For Snowpack, in order to find one packet, we need to find the F fragments corresponding to it. We do all the combinations.

$$O \sim N^F$$

By assuming that a computer can test one billion combinations per second

Time to crack	N = 10	N = 100	N = 1000	N = 10000	N = 100000
F = 2	~instant	~instant	~instant	~instant	~instant
F = 3	~instant	~instant	1 s	16 m	11 d
F = 4	~instant	~instant	16 m	115 d	3170 y
F = 5	~instant	10 s	11 d	3170 y	317M y

With N equal to 100000 packets and the average IP packet size (576 bytes), the sum of all traffic rate from clients should be 57.6 Mbyte/s.

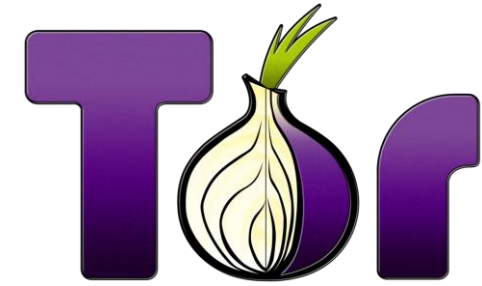


Snowpack: easier and superior to other general-purpose solutions

	Snowpack	VPN	Tor	I2P net.	JonDonym	Nym
<u>Delivers privacy</u>	✓	✓	✓	✓	✓	✓
No trusted third party	✓	x	x	x	x	x
Immune to basic traffic basic analysis	✓	x	✓	✓	x	?
Immune to AI-based traffic analysis	✓	x	x	x	x	?
Node integrity guarantees	✓	x	x	x	x	x
Low latency dependency	✓	x	x	x	x	x
Access control	✓	✓	x	x	x	✓
Supports all IP protocols	✓	✓	x	x	✓	?
<u>Delivers security</u>	✓	✓	x	x	x	x
Immune to MITM	✓	x	x	x	x	x
Forward secrecy	✓	x	x	x	x	x
QoSec increases with users	✓	x	x	x	x	x
Hides surface attack	✓	x	x	x	x	x
<u>Additional features</u>						
Routes	<i>Dynamic</i>	<i>Static</i>	<i>Random</i>	<i>Random</i>	<i>Static</i>	<i>Random</i>
Active counter-measures	✓	x	x	x	x	✓
Mass surveillance proof	✓	x	x	x	x	x
Protects against availability attacks	✓	x	x	x	x	x
Easy to use	✓	✓	x	x	x	✓
Agility	✓	x	x	x	x	x
QoS	<i>Dynamic</i>	<i>Static</i>	x	x	<i>Static</i>	<i>Static</i>



Snowpack vs TOR



Tor (originally called **The Onion Router** because it layers your traffic like an onion) is a free network of Peer to Peer servers (nodes) that randomly route internet traffic between each other in order to obfuscate the origin of the data. The Tor Browser can significantly increase a user's privacy and anonymity online. In internal documents, the NSA has even referred to Tor as "the king of high-secure, low-latency internet anonymity."

Snowpack is here to replace the king, because Snowpack is more ethical, more secure and more performant, the three problems of Tor.

- **Ethical:** over 50% of Tor activity is criminal or related to illegal uses
- **Secure:** 24% of Tor exit nodes perform attack on the data
- **Performance:** Peer to Peer means QoS is poor and bandwidth is (very) bad

Snowpack solves all these problems:

- **Ethical:** Snowpack logs in FreeSnow and OneSnow plans and uses strong KYC for DarkSnow and ProSnow
- **Secure:** Snowpack brings a new dimension of security (even Snowpack can not see the data, when the exit nodes of Tor can see and attack it)
- **Performance:** Up to 100 Mb/s bandwidth (and soon 1 Gb/s), QoS over 99%, support service available



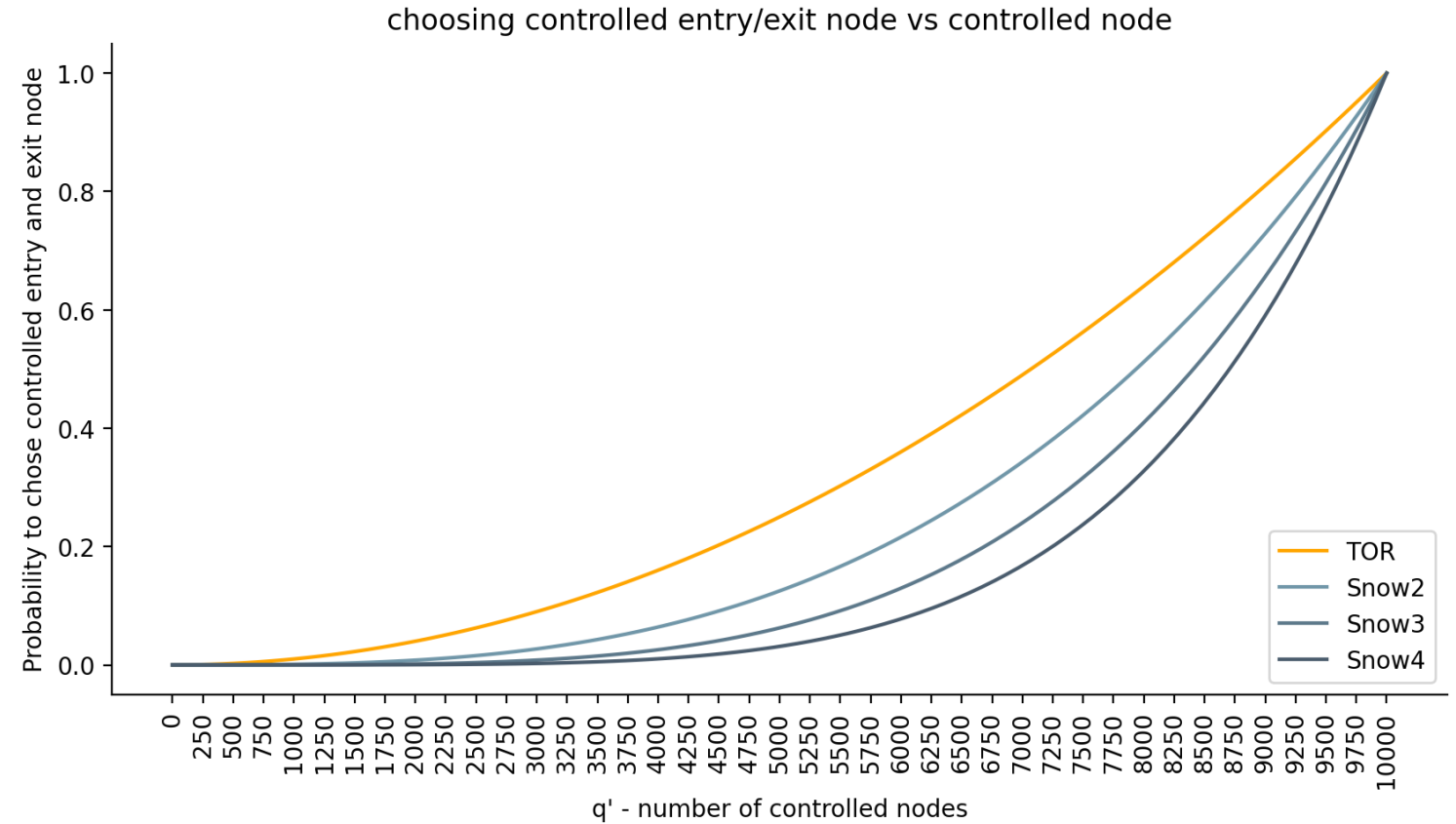
Quantitative comparative analysis to TOR

$$C_{tor} = \frac{0,4 * N_b}{4000} * \frac{0,1 * N_b}{10000} = \left(\frac{N_b}{10000}\right)^2$$

Probability to choose controlled entry/exit node in TOR

$$C_{snow_F} = \left(\frac{N_b}{10000}\right)^{F+1}$$

Probability to choose controlled entry/exit node in SnowF



By assuming that TOR is composed of 4000 entry relays, 1000 exit relays and 5000 other relays (same basis for snowpack)



Snowpack vs VPN



A virtual private network (**VPN**) extends a private network across a public network like Internet and enables users to send and receive data as if their devices were directly connected to the private network. VPNs are used with encryption of the data and are very common for Professional and Personal uses. They mainly suffer from some strong limitations:



- **Insufficient Privacy** as your Internet Service Provider and State see your connection to the VPN servers
- **Need to Trust:** your VPN provider is a trusted third-party (even if they pretend not to log, they most often do log, and are attacked, hacked or cracked)
- **Ethical:** VPN are playing on the ethical borders (especially when used with Tor to provide a protection to connect to Tor privately) and illegal uses are common

Snowpack is a much better solution than a VPN:

- **Private** (and Secure): your data are hidden in randomly generated noise in your device and then into the traffic of all users so that you are truly private and secure
- **No-Trust:** with ProSnow, you don't need to trust anyone (even Snowpack) since you are immersed in our Snowpack Network Overlay
- **Ethical:** Snowpack logs (under the French and EU law) for FreeSnow and OneSnow plans and uses strong KYC for DarkSnow and ProSnow, diminishing greatly illegal and criminal uses



Snowpack short-term roadmap

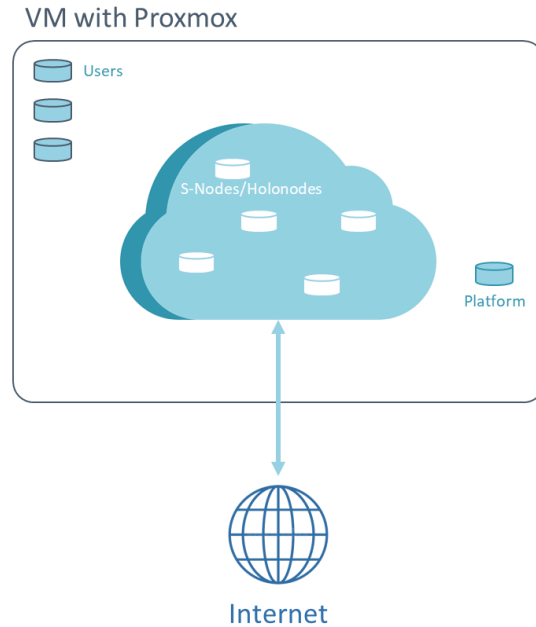
	Q1 2022	Q2 2022	Q3 2022	Q4 2022	Q1 2023
	Backup route Traffic segregation	Suggestive route system	Advanced Noise Generator	Advanced Suggestive route system	Mobile client AI based noise generator
	100 Mbit/s	1 Gbit/s Additional latency < 0.2ms Security Mode Without preshared key	Anonymous access control Snowpack SOC Proof-of-work (partner remuneration while processing others traffic)	+10 Gbit/s Additional latency < 0.05ms Remote attestation of node code Decentralized platform	Fail-over Snowpack Certification



Testing & deploying



Environment – vSnowpack



This environment can be available to partners & clients through traditional Internet network via a VPN access.

Or with on-premise dedicated machine.

To proceed a test with up to 40 (nodes + users) running at the same time, the recommended configuration should be equivalent to:

Processor : AMD Epyc 7413 – 24c / 48 t – 2.65GHz / 3.6GHz

Memory : 128 Go DDR4 ECC 3200MHz

Storage : 2 x 960 Go SSD NVMe Soft RAID

Running a Proxmox server version > 6.4



Environment – vSnowpack

vSnowpack consists in the emulation of a fully operational Snowpack network inside a Proxmox environment.

The environment natively embeds:

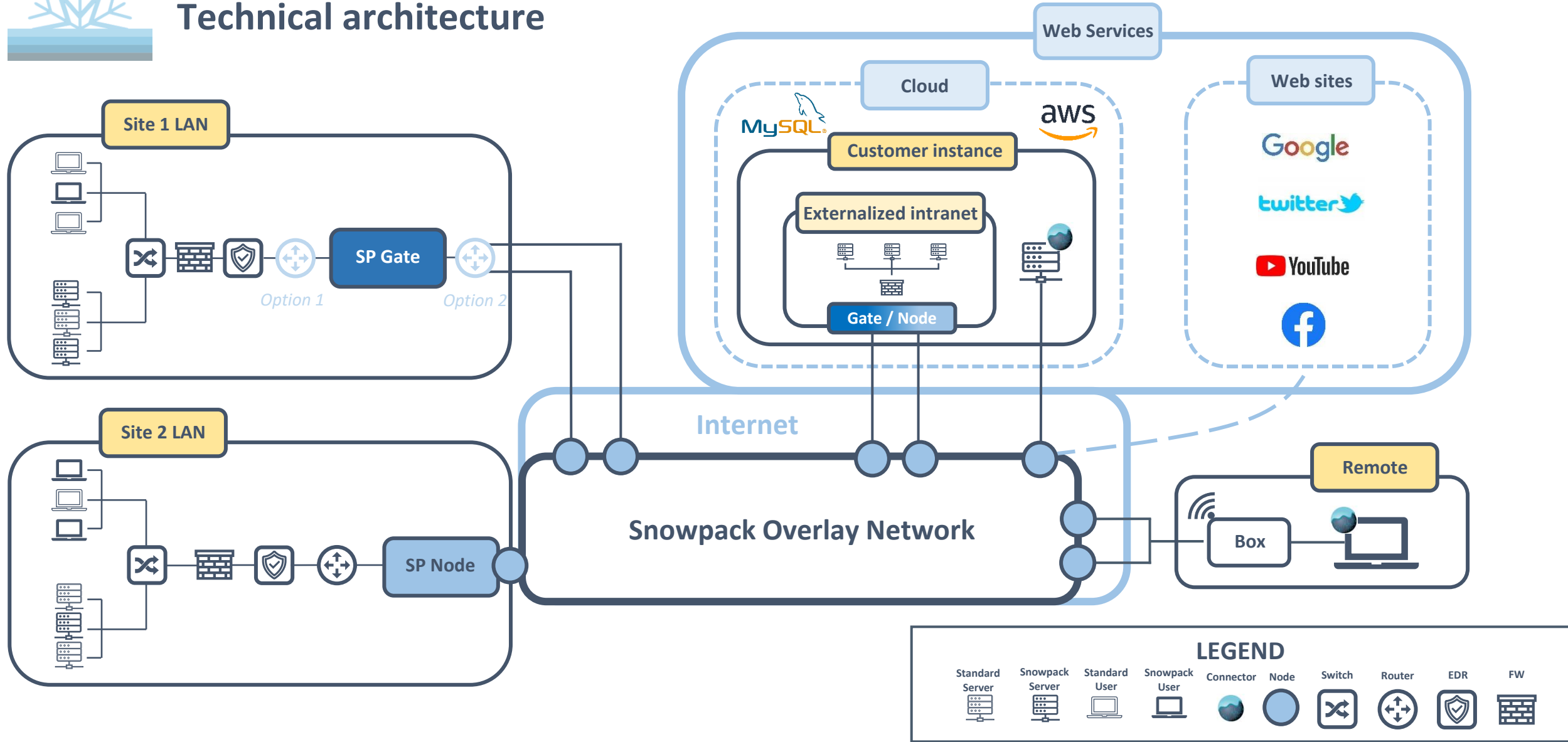
- The management platform
- LXC template for S-nodes and holonodes
- LXC template for Snowpack connectors without GUI
- VM template for Snowpack connectors with remote GUI
- Scripts to generate Snowpack nodes and users
- Script to simplify the set up/set down of nodes and users
- Script to proceed ping, wget and speedtest

Additional features can be added:

- Script to retrieve all snowpack logs
- Script to launch/stop a network probing
- Script to define the latency and drop rate between each LXC

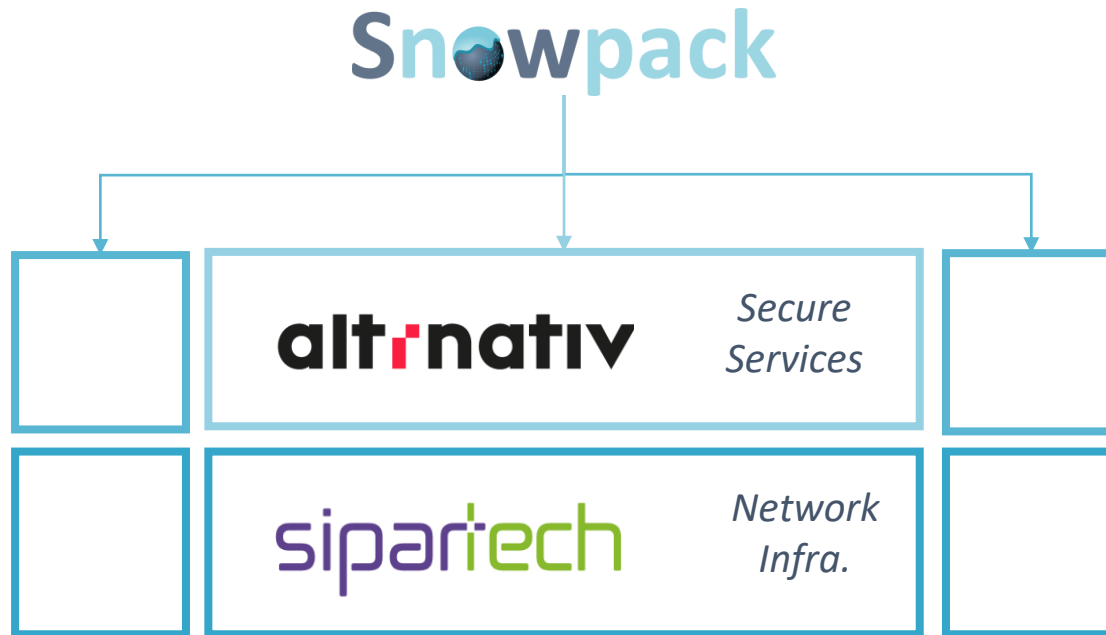


Technical architecture





SNO is already up and running (alpha) with Altrnativ



Snowpack users do not need to trust Snowpack, Sipartech or Altrnativ (nor their ISP)

>50 servers
12 datacenters
6 European Countries (Q1 2022)
Partnerships with other cloud providers





SNO is already up and running (alpha) - Plans

FreeSnow and OneSnow for

- Brand awareness
- Network noise

DarkSnow for

- Intel. & Counter Intel
- Investigations
- Cyberdefense

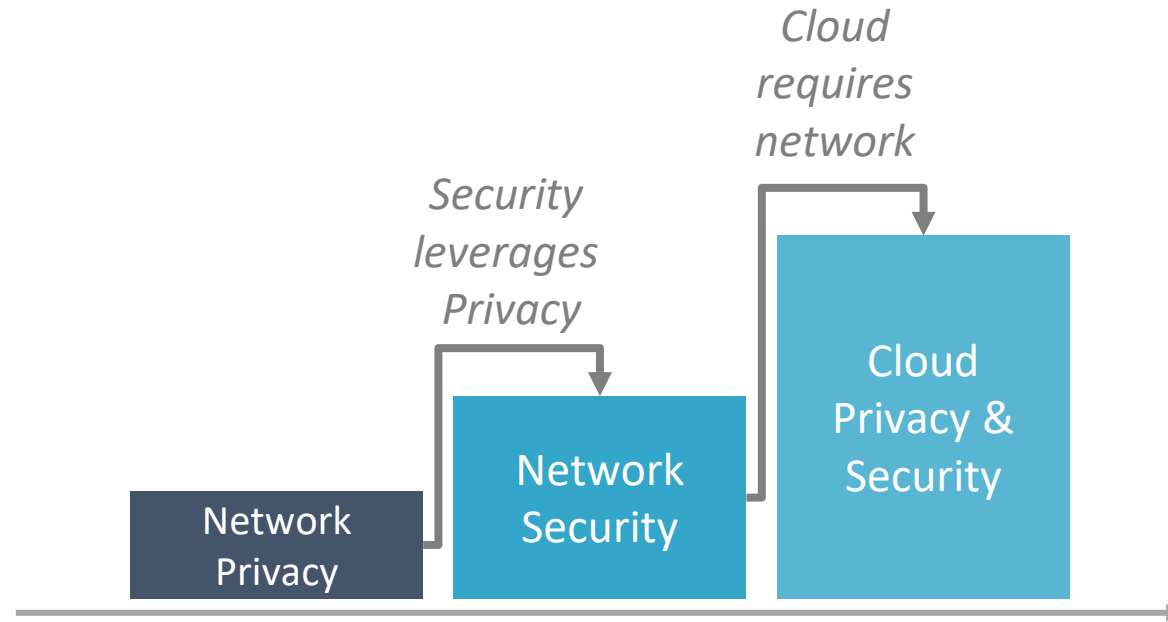
ProSnow for

- Large corporation
- Critical infrastructures
- Sensitive SMEs

FreeSnow	OneSnow	DarkSnow	ProSnow
0€ / Month	9€ / Month	29€ / Month	Ask us
The perfect solution to start reducing your exposure on internet while browsing. Let's become invisible !	For Individuals, SMEs wanting to take care of their privacy on all there day to day Internet access	For Investigators , Economic Intelligence, Cyber Experts requiring high level of privacy to proceed their jobs	For Companies, Institutions, Governments wanting to take full power of SNO
<ul style="list-style-type: none">✓ 1 GB/day✓ HTTP browsing✓ Automatic route definition✓ Protection against Hackers✓ Protection against Foreign state✓ Classical browsing (including UDP)✓ Darknet access✓ Refined route definition✓ PRO route definition✓ Protection against your ISP✓ Protection against your local state	<ul style="list-style-type: none">✓ 10 GB/day✓ HTTP browsing✓ Classical browsing (including UDP)✓ Automatic route definition✓ Refined route definition✓ Protection against Hackers✓ Protection against Foreign state✓ Darknet access✓ PRO route definition✓ Protection against your ISP✓ Protection against your local state	<ul style="list-style-type: none">✓ Unlimited✓ HTTP browsing✓ Classical browsing (including UDP)✓ Darknet access✓ Automatic route definition✓ Refined route definition✓ PRO route definition✓ Protection against Hackers✓ Protection against Foreign state✓ Protection against your ISP✓ Protection against your local state	<ul style="list-style-type: none">✓ Unlimited✓ HTTP browsing✓ Classical browsing (including UDP)✓ Darknet access✓ Automatic route definition✓ Refined route definition✓ PRO route definition✓ Protection against Hackers✓ Protection against Foreign state✓ Protection against your ISP✓ Protection against your local state



Snowpack Markets Penetration Strategy



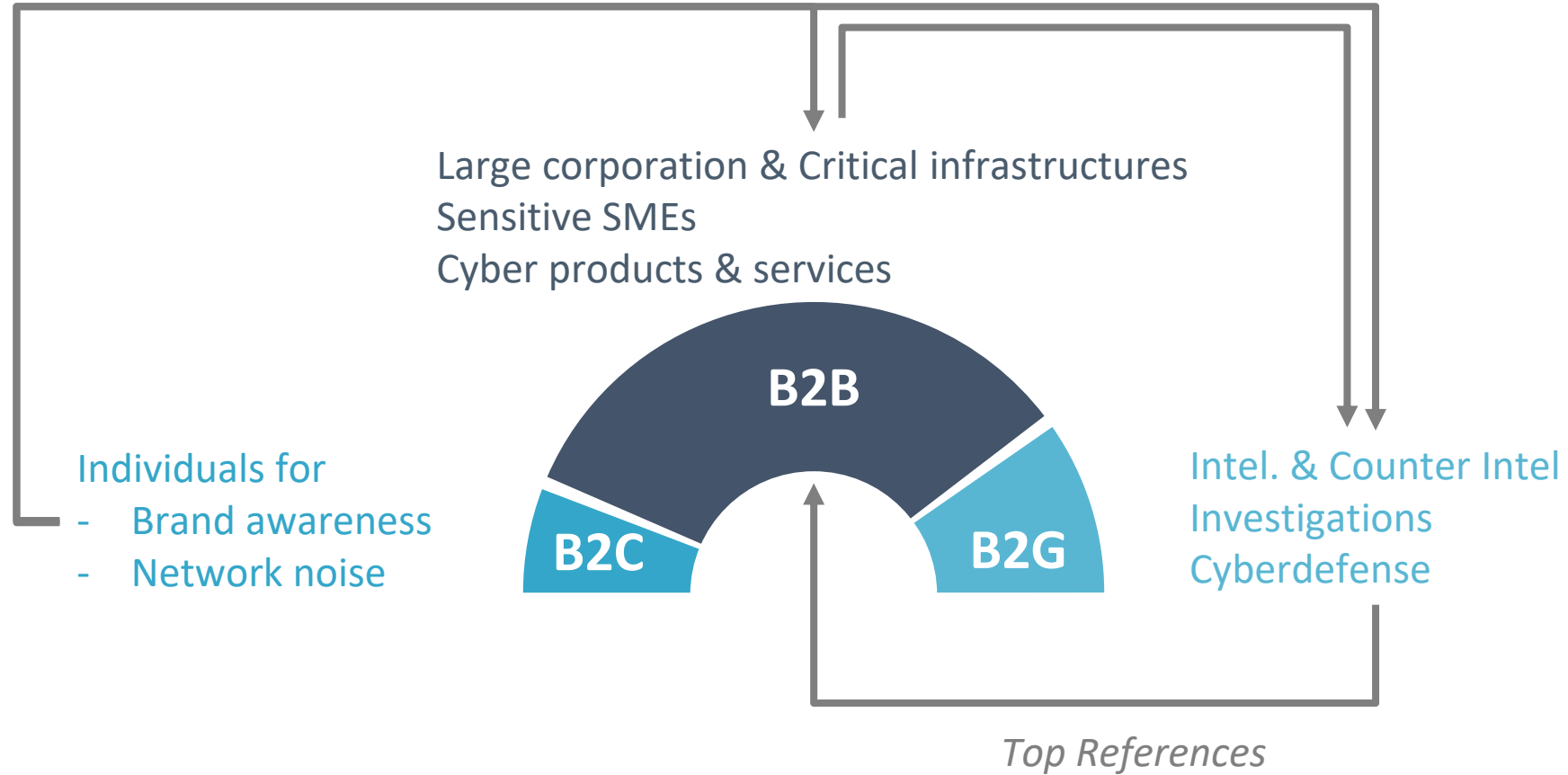
Different Advantages of SNO lead to different value propositions:

- Privacy
- Security
- Cloud



Snowpack End-users

Increase Privacy & Security properties AND marketing reach





Thank you

Contact: frederic.laurent@snowpack.eu