Protecting Insecure Communications with Topology-aware Network Tunnels

Georgios Kontaxis Angelos D. Keromytis

Department of Computer Science
Columbia University, USA

Clients securing their traffic to a server

- TLS unavailable at the server
- Minimize the unencrypted network path on the Internet
- Without the server's participation
- Not a substitute for TLS!

Limited adoption of transport layer security

- Top 10K sites (Alexa)
- Only 32% support HTTPS
- Only 15% redirect HTTP to HTTPS

	HTTPS response	HTTPS?	%	#
1	Error (Conn. refused)	No	21.4	2144
2	Error (Invalid cert.)	No	22.1	2205
3	Error (HTTP 4xx 5xx)	No	2.9	292
4	HTTPS downgraded	No	21.5	2152
	Total	No	67.9	6793
5	OK	Yes	17.0	1695
6	OK (HTTP upgraded)	Yes	15.1	1512
	Total	Yes	32.1	3207

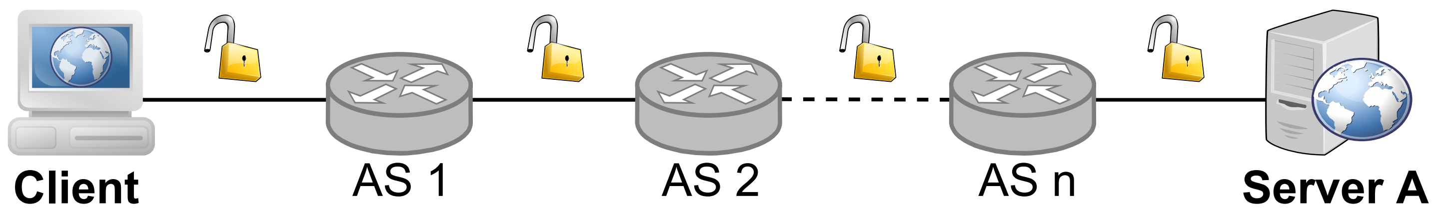
Imperfect deployment of TLS

- Implementation vulnerabilities threaten user security

FREAK	POODLE	Heartbleed	RC4
BEAST	DROWN		

- Users cannot rely on websites to patch themselves up
  - 45% of servers affected by FREAK vulnerable 9 months later
  - DROWN affects a TLS 1.2 client because server supports SSLv2

Short network paths minimize the attack surface



- kontaxis@austria$ traceroute www.nytimes.com
    1. EDIS GmbH (AT)
    2. RETN Limited (UK)
    3. NTT America, Inc. (US)
    4. Fastly (US)

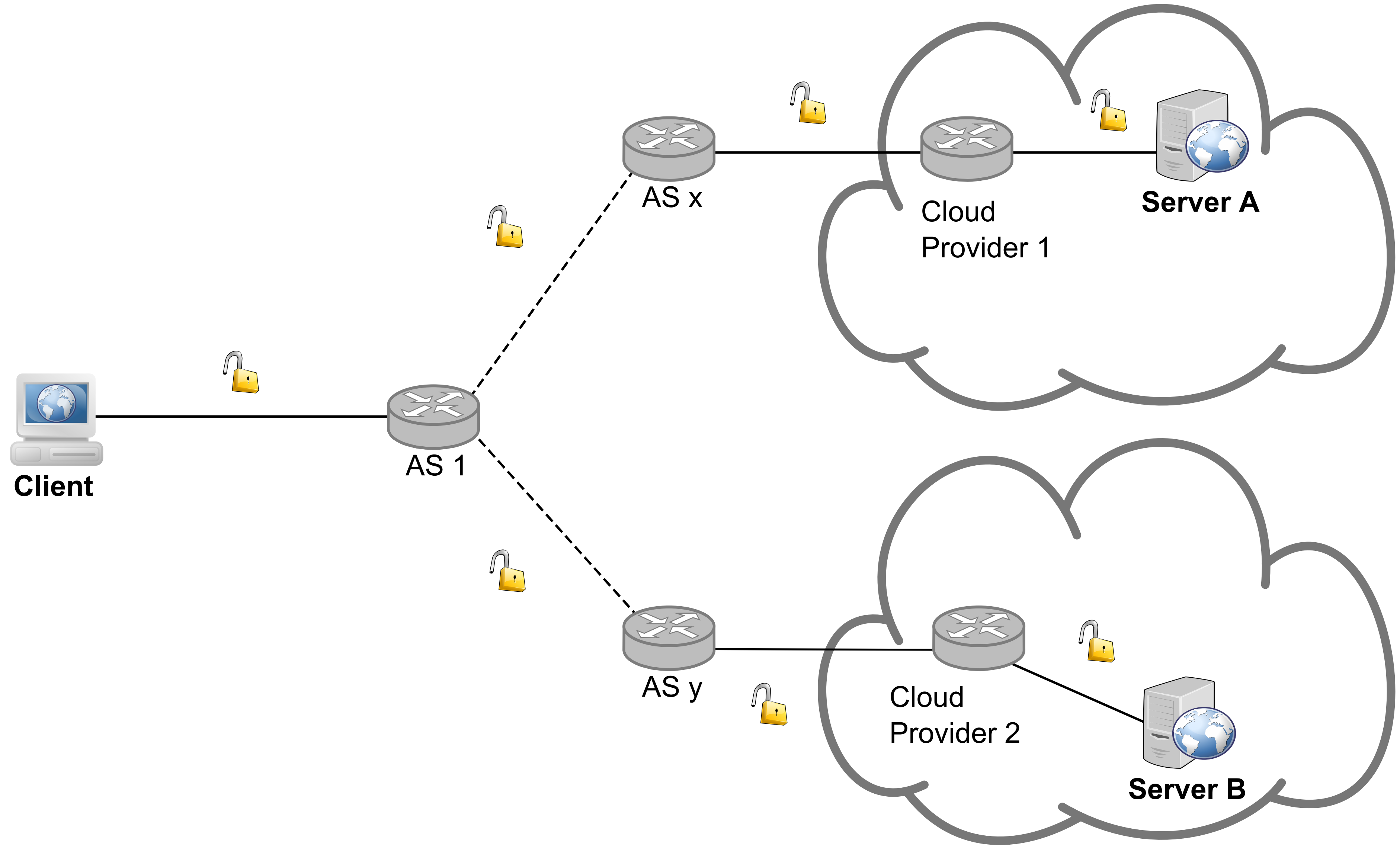
- kontaxis@ec2-us-east-1$ traceroute www.nytimes.com
    1. Amazon Inc. (US)
    2. Fastly (US)

Web services are clustered in the cloud

- Cloud networks host the majority of web services
- Excellent vantage point to browse the web
- Users have access to Virtual Machines in the cloud

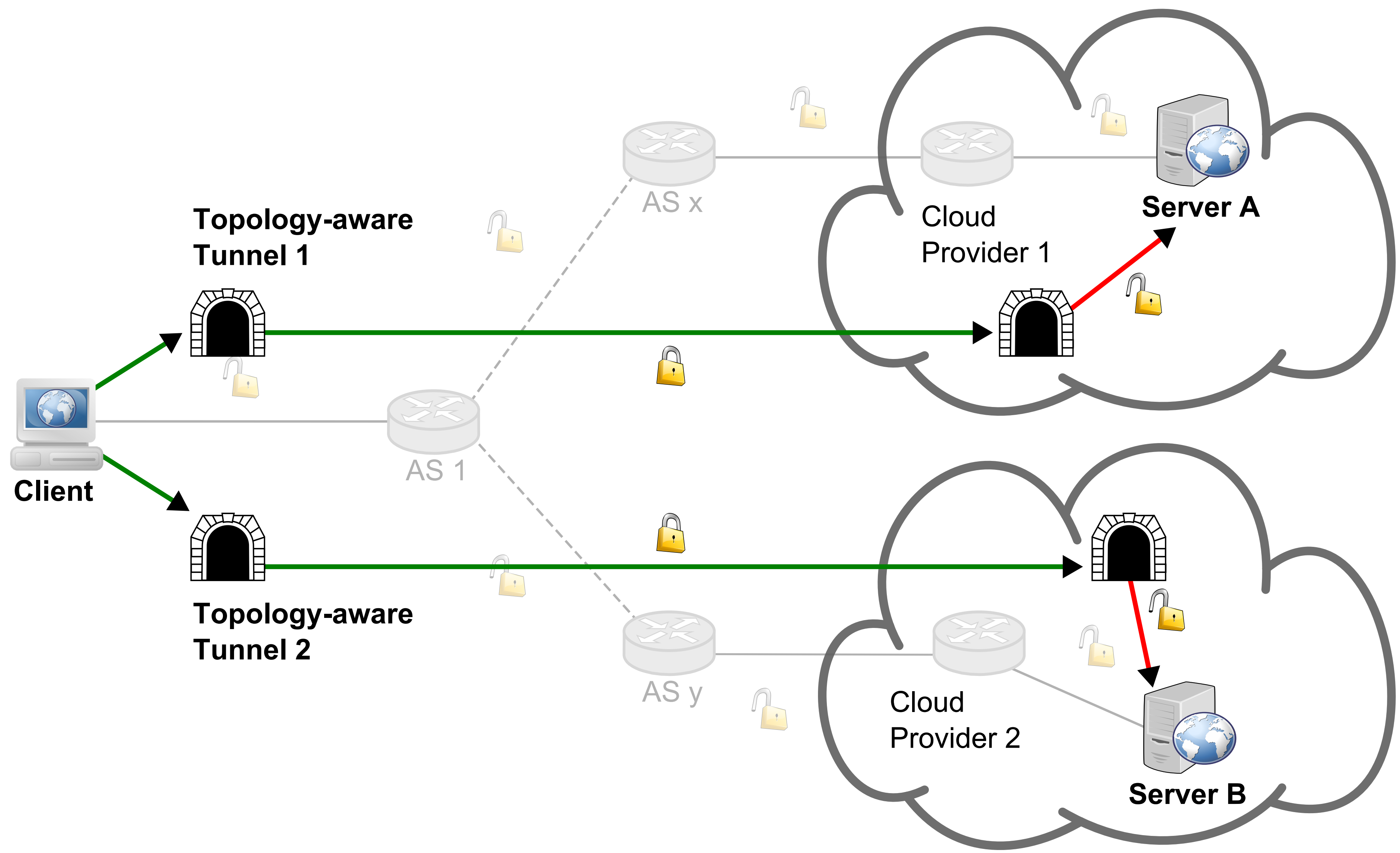
%	Autonomous System Name
17.1	Akamai Technologies, Inc.
13.9	Amazon.com, Inc.
11.4	CloudFlare, Inc.
9.9	Google Inc.
3.7	EdgeCast Networks, Inc.
2.9	SoftLayer Technologies Inc.
2.1	Fastly
1.7	Tinet SpA
1.6	Internap Network Services Corp.
1.5	Rackspace Hosting
65.8	Total

Cloud networks are the gateway to Internet services



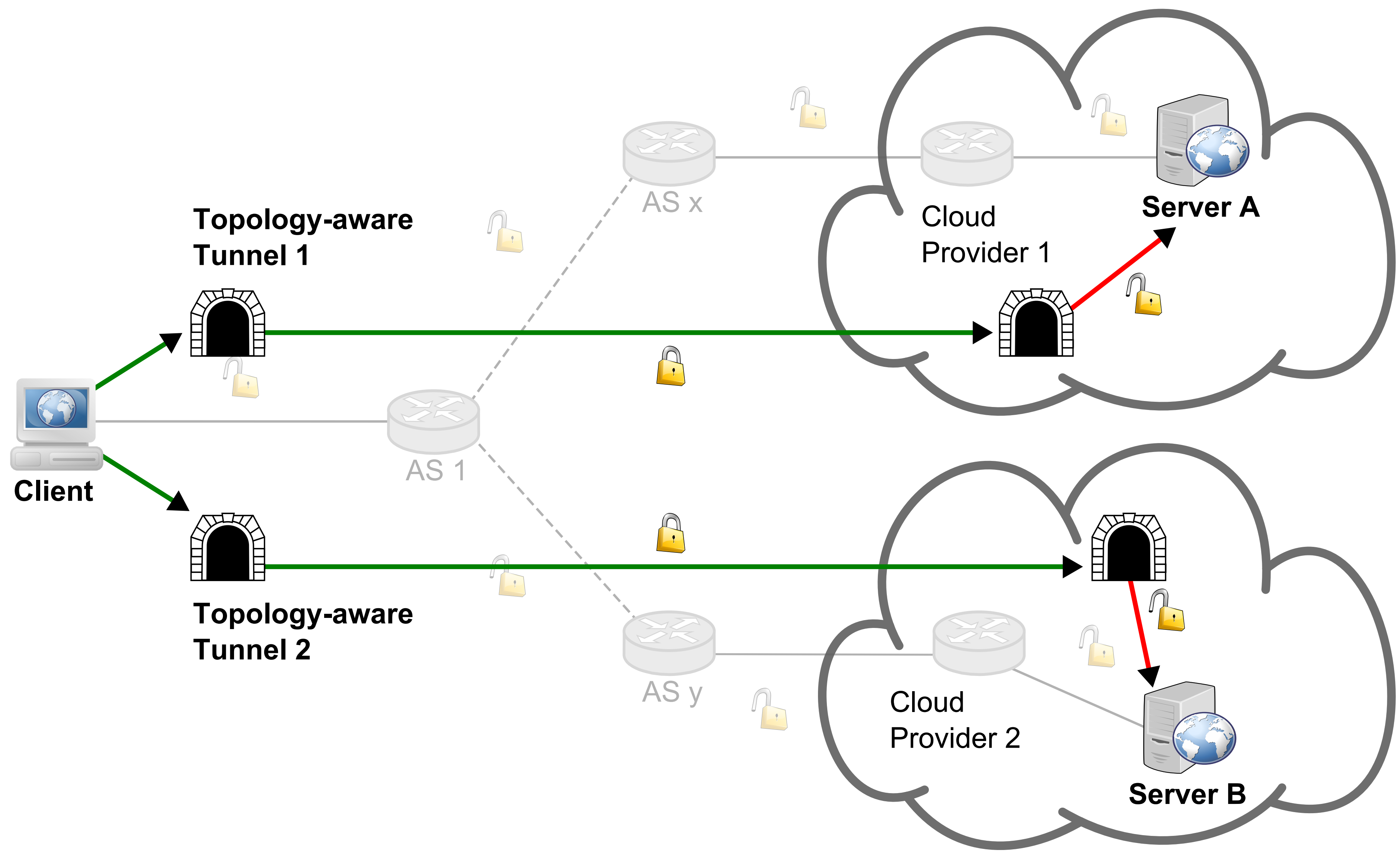
Proposed overlay of encrypted tunnels with the cloud

- We replace multi-hop plain-text links with encrypted tunnels

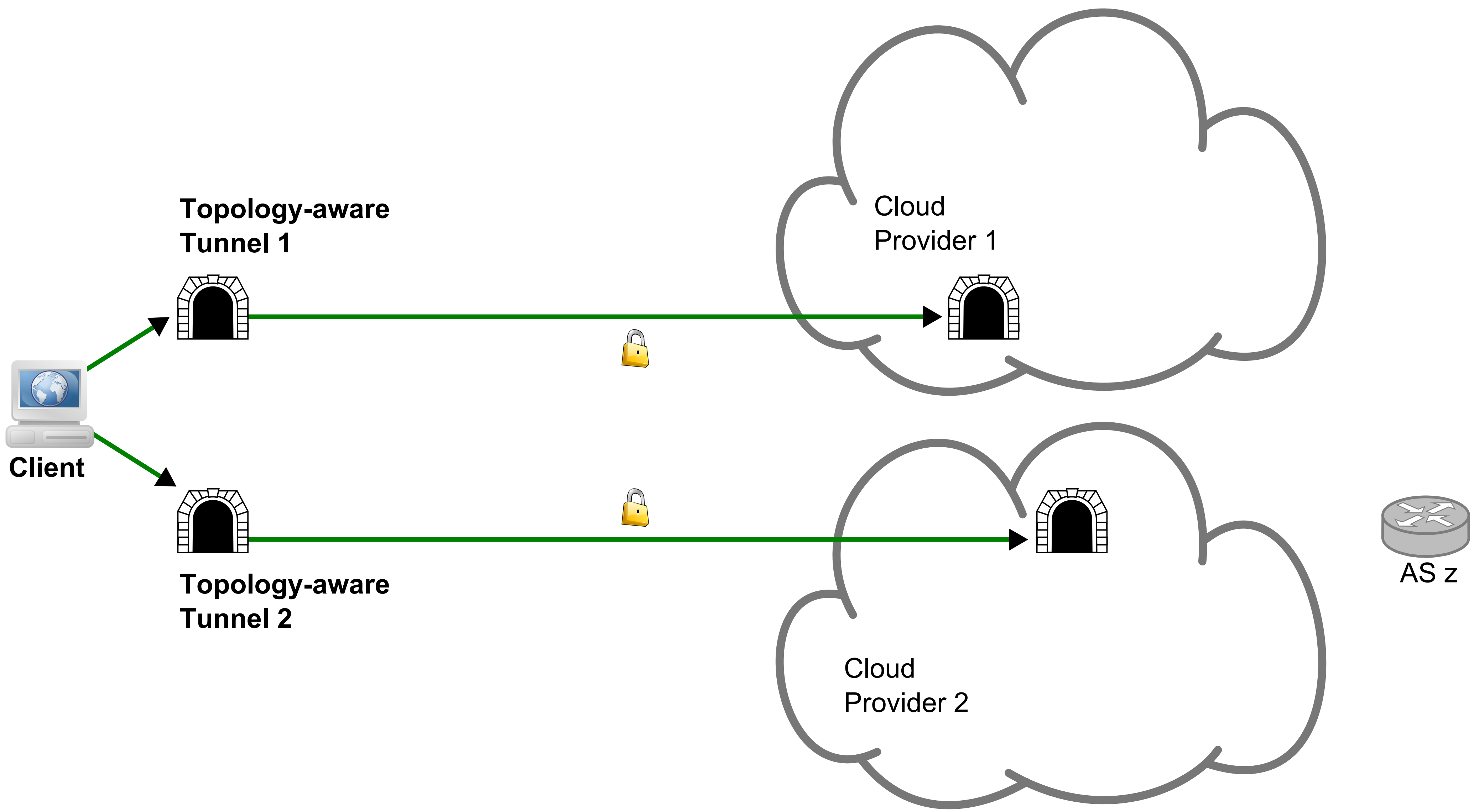


Topology-aware Network Tunnels (TNT)

- Routing through the tunnel closest to the server



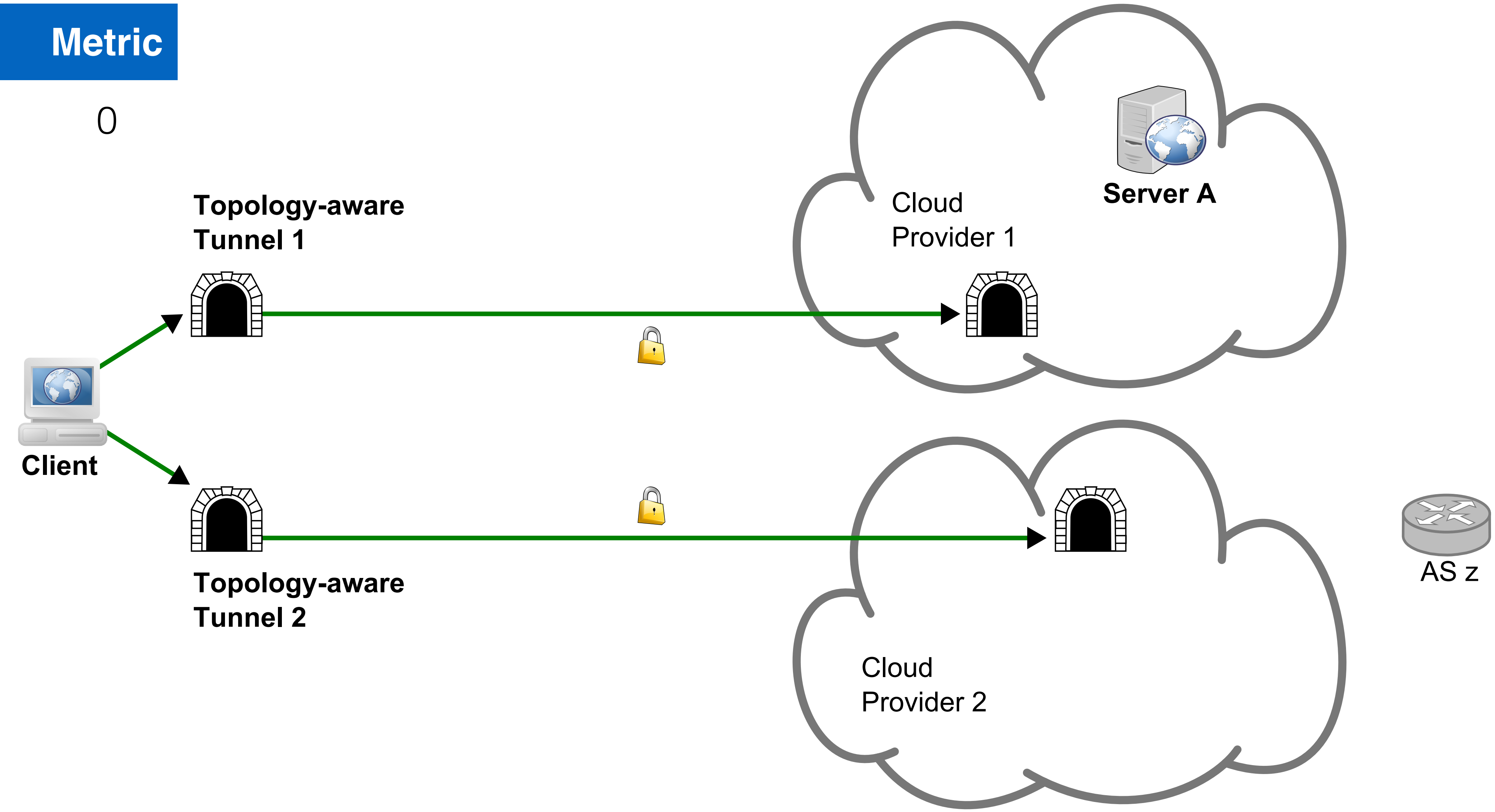
TNT establishes links to popular cloud networks



Given a destination TNT maps the available paths

- Initially traffic is routed through a tunnel at random

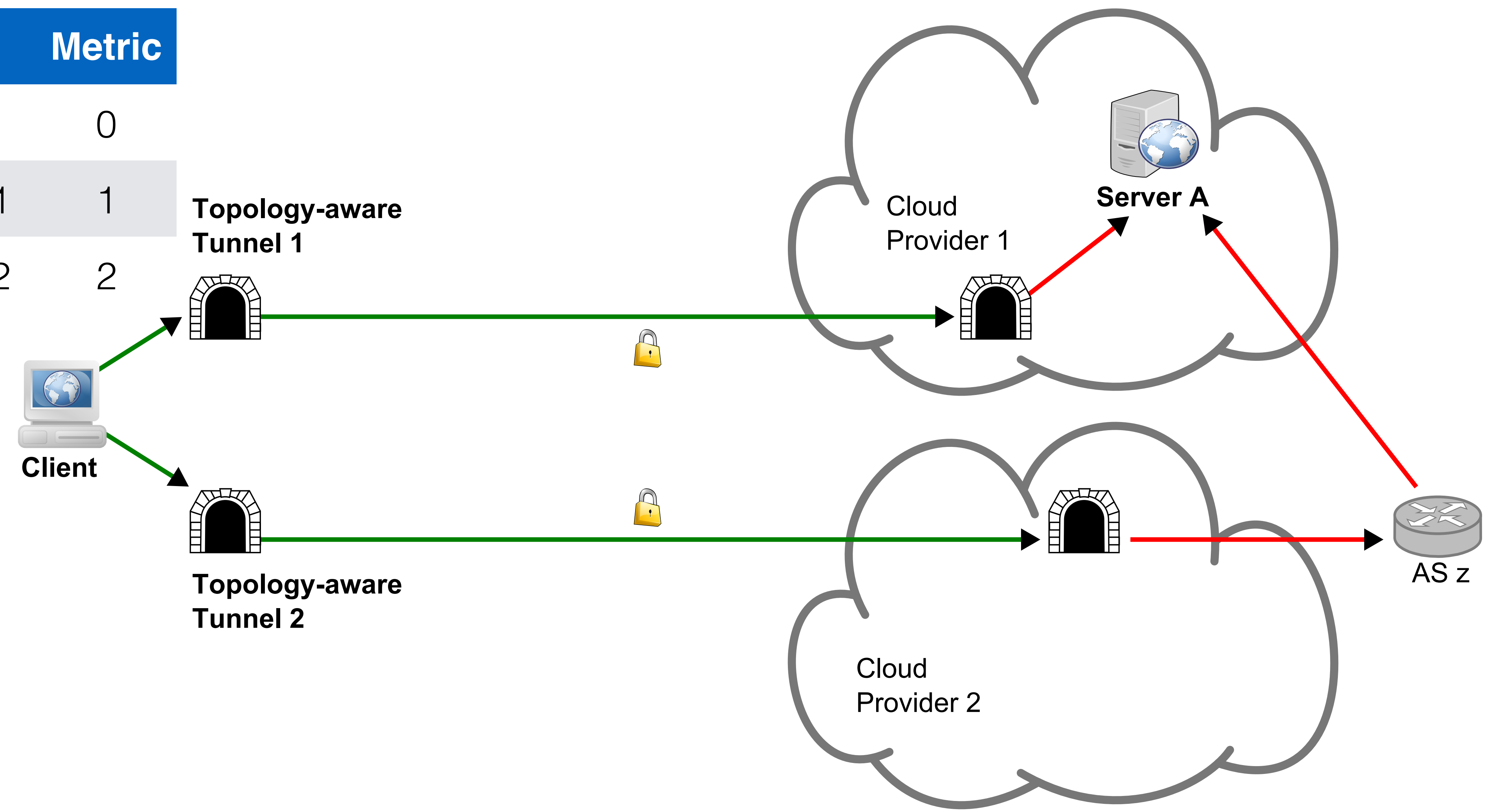
Dest	GW	Metric
Any	Any	0



TNT evaluates the available paths to a destination

- Active, passive network measurements identify the shortest path

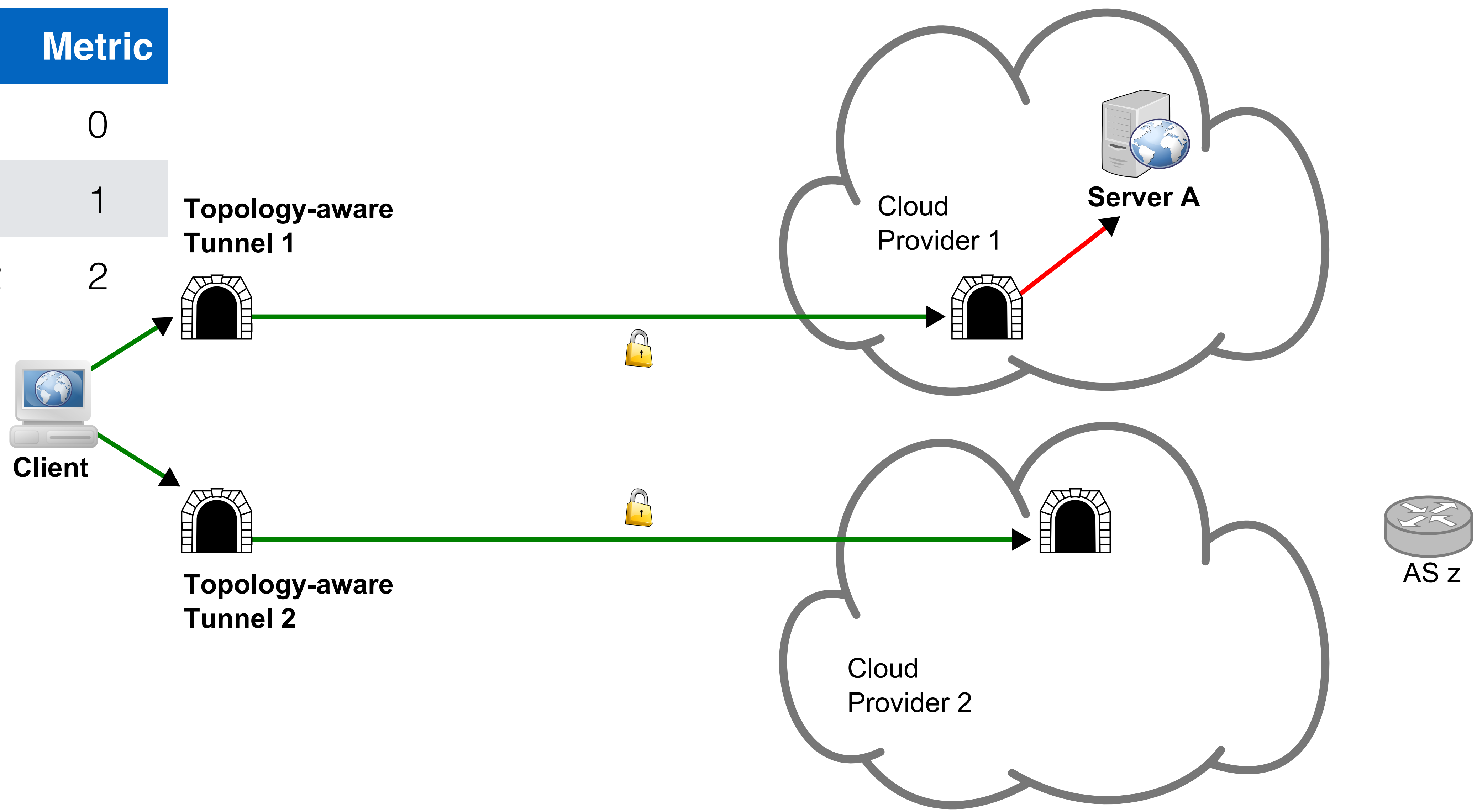
Dest	GW	Metric
Any	Any	0
A	Tun 1	1
A	Tun 2	2



TNT makes routing decisions to minimize plain-text traffic

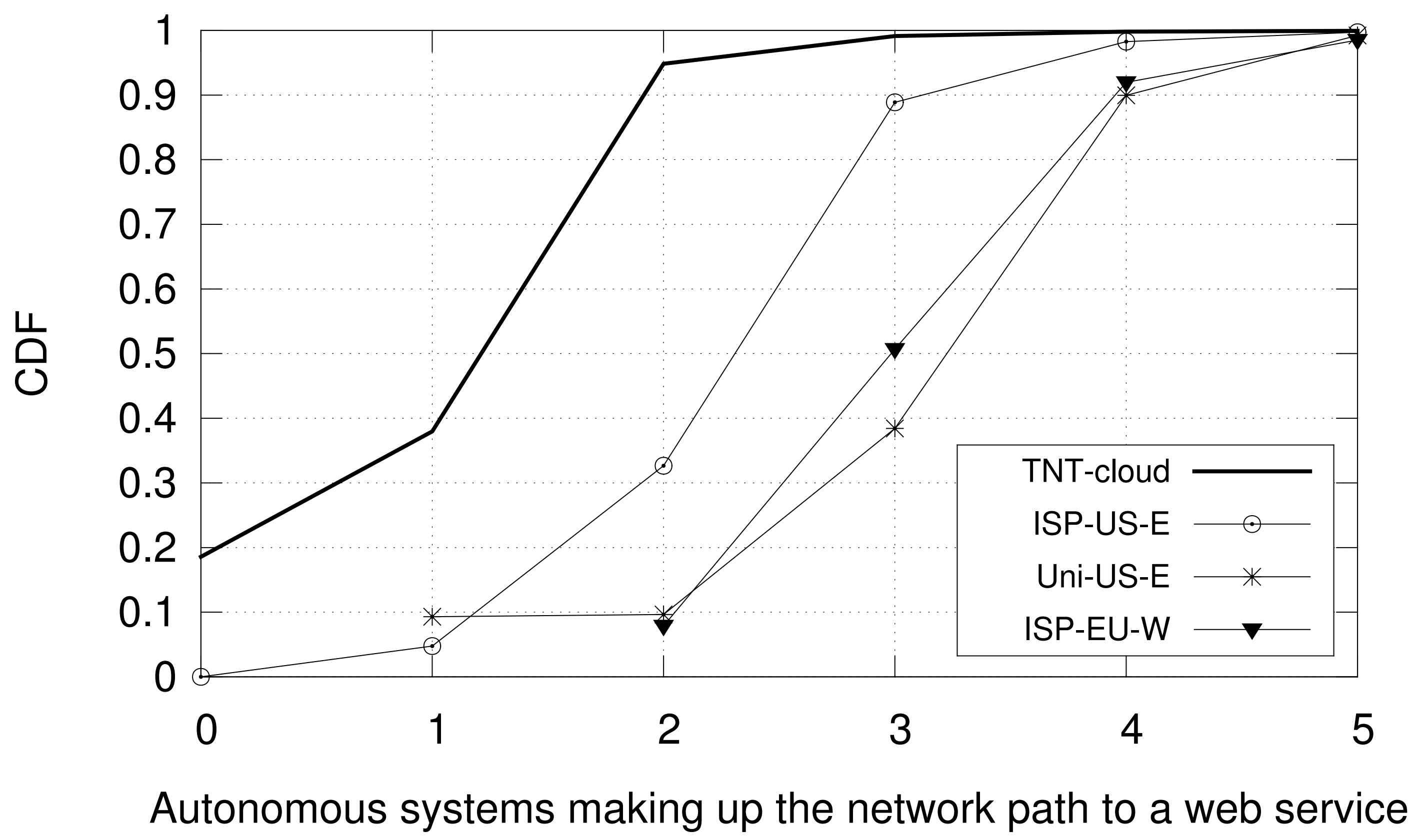
- TNT starts routing packets through the shortest path in real time

Dest	GW	Metric
Any	Any	0
A	Tun 1	1
A	Tun 2	2



Insecure network paths are minimized

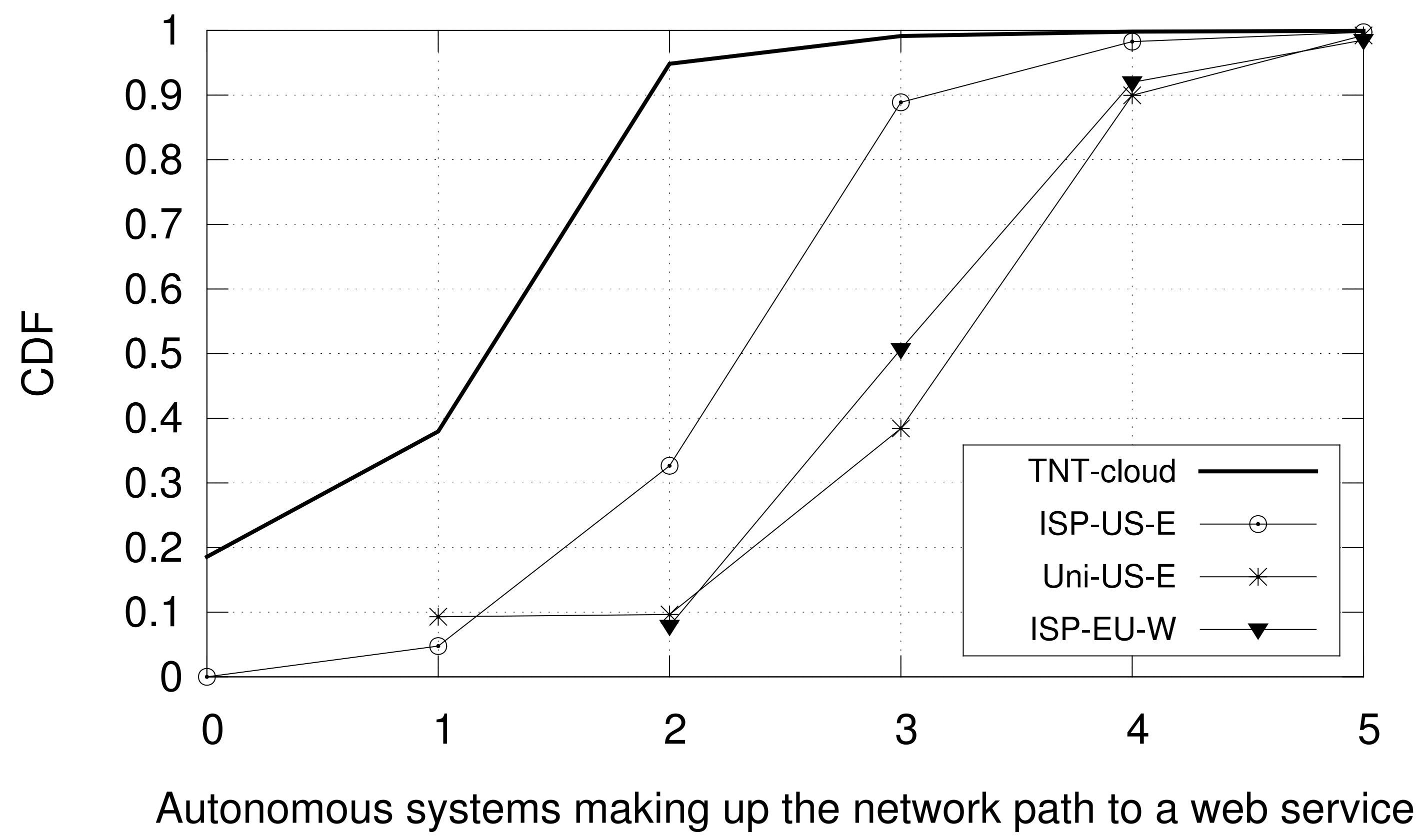
- Tunnel exit in the same network as a web server
  - Zero traffic exposure to the Internet
- Tunnels to AWS, Azure are colocated with 20% of web services



kontaxis@cs.columbia.edu

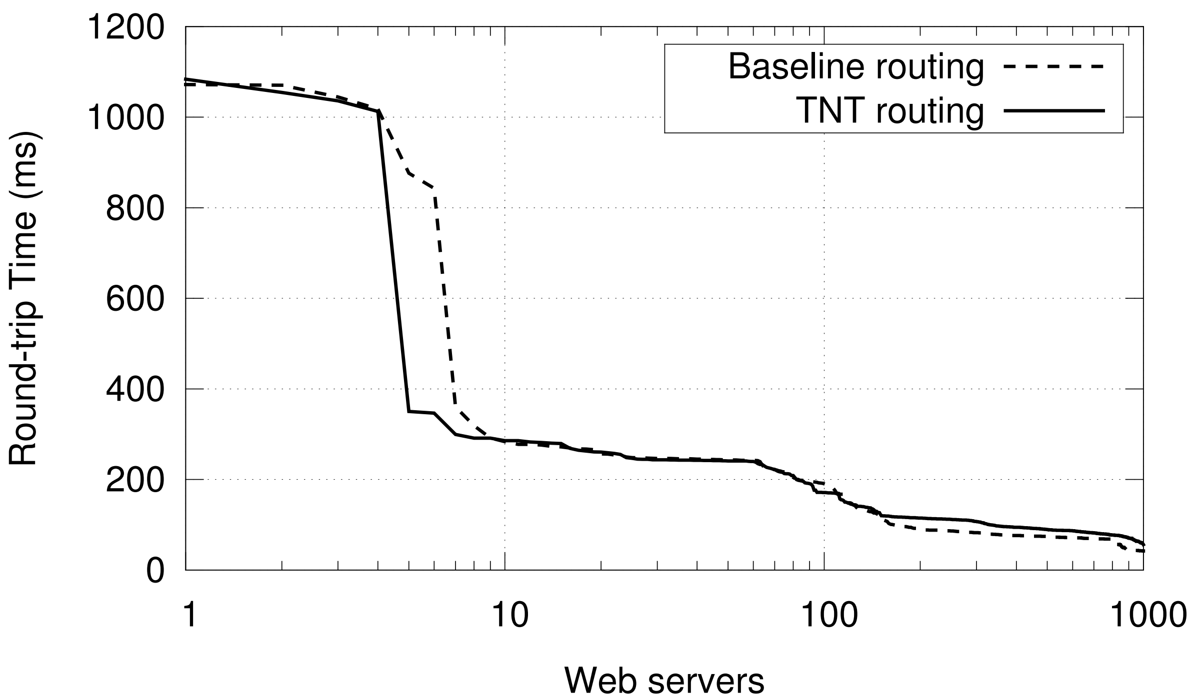
Insecure network paths are minimized

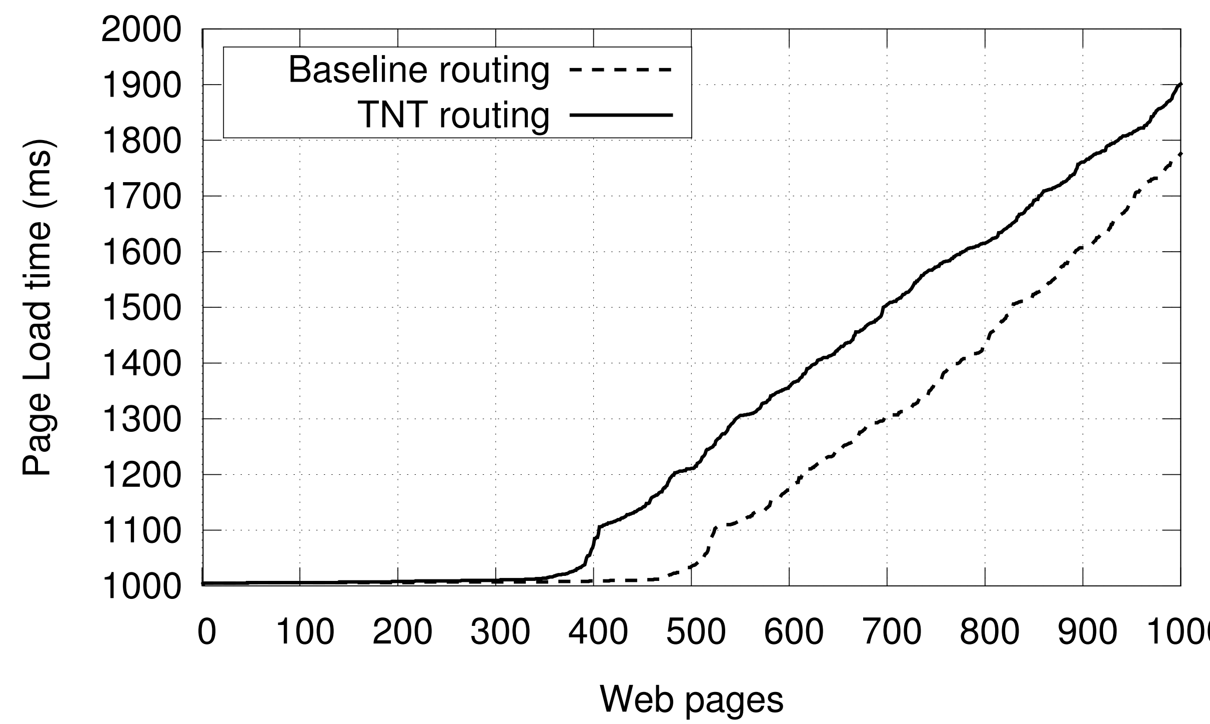
- Tunnel exit in a network near the web server
    - Minimal traffic exchange outside the cloud
- TNT paths are always shorter than the native path



TNT preserves the browsing experience

- Page load time and latency do not deviate from the baseline
- Used the network at Columbia University for comparison





Topology-aware network tunnels

- An overlay of encrypted links to key network infrastructure
- Motivated by the clustering of services in the cloud
- Minimize plain-text traffic on the Internet
- Without the cooperation of individual services
- Put clients in control of their security
- Deployable using existing technologies and resources

Find out more about TNT

https://www.cs.columbia.edu/~kontaxis/tnt/

kontaxis@cs.columbia.edu