Path aware routing over MASQUE proxies

Tommy Pauly
PANRG
IETF 111, July 2021, Virtual

Background

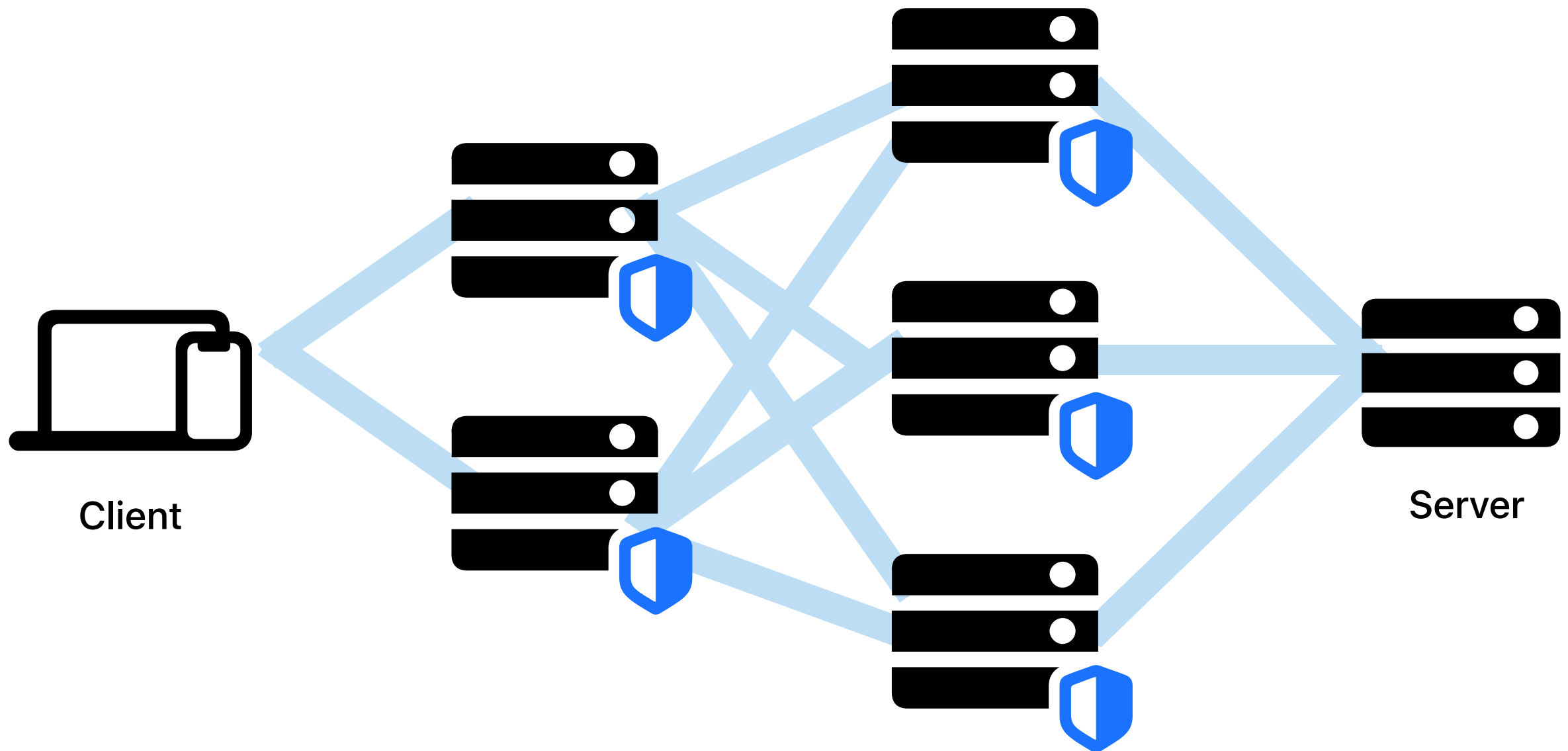iOS 15 and macOS Monterey add support for iCloud Private Relay

Solution for user privacy that separates client IPs from origin servers

Multi-hop MASQUE proxies

Oblivious DoH for other traffic

So why is a privacy proxy relevant for path-aware networking?

Client

Server

Privacy benefits of path awareness

Clients learn about a diverse set of proxy hops

Control over which hops are used, validated by secure handshakes with each hop

Separation of data between hops improves privacy

Selection of different paths over time ensures data can't be aggregated by one provider

Performance benefits of path awareness

Egress proxies can be selected to be co-located with content

Currently using several major CDN providers

Clients can switch between proxy paths

Measure performance on each combination, etc

Connections can migrate between paths without breaking end-to-end connectivity

Proxies don't need to be slow

Proxied connections can always "fast open"

"QUIC-aware"[1] proxies can forward connections without re-encapsulation

Proxy ends up being an authenticated NAT/router that supports connection migration

Forwarding path can be highly efficient (eBPF offload, etc)

1. https://www.ietf.org/archive/id/draft-pauly-masque-quic-proxy-01.html

Areas for new work

Discovery of proxies/paths

Discovery of which hosts are associated with a specific egress

Migration and traffic splitting strategies

A future vision

Ingress proxies hosted by ISPs

Specialized proxies could support zero-rating, slicing, etc

Egress proxies hosted by CDNs

Overlay network that allows path selection, while improving privacy

Thoughts?