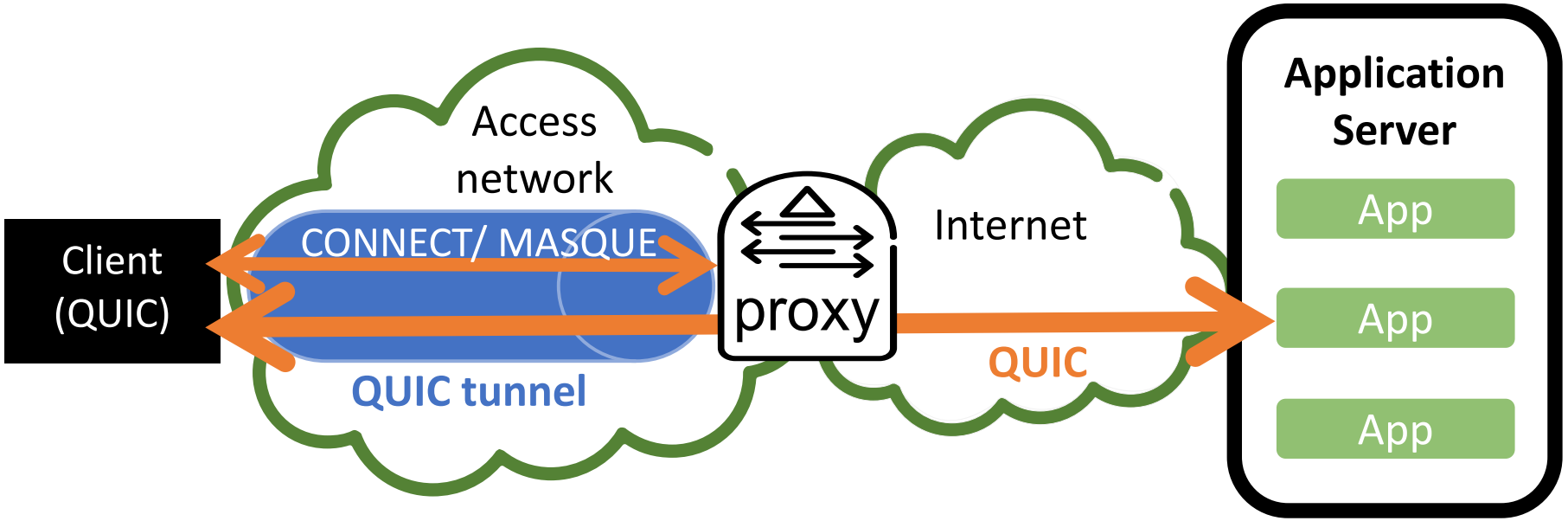
Use Cases and Requirements for QUIC as a Substrate

Goal

- Use QUIC as substrate/tunnelling protocol to proxies/VPN server/load balancers…
  - Utilize QUIC's ability to multiplex, encrypt data, and migrate between network paths

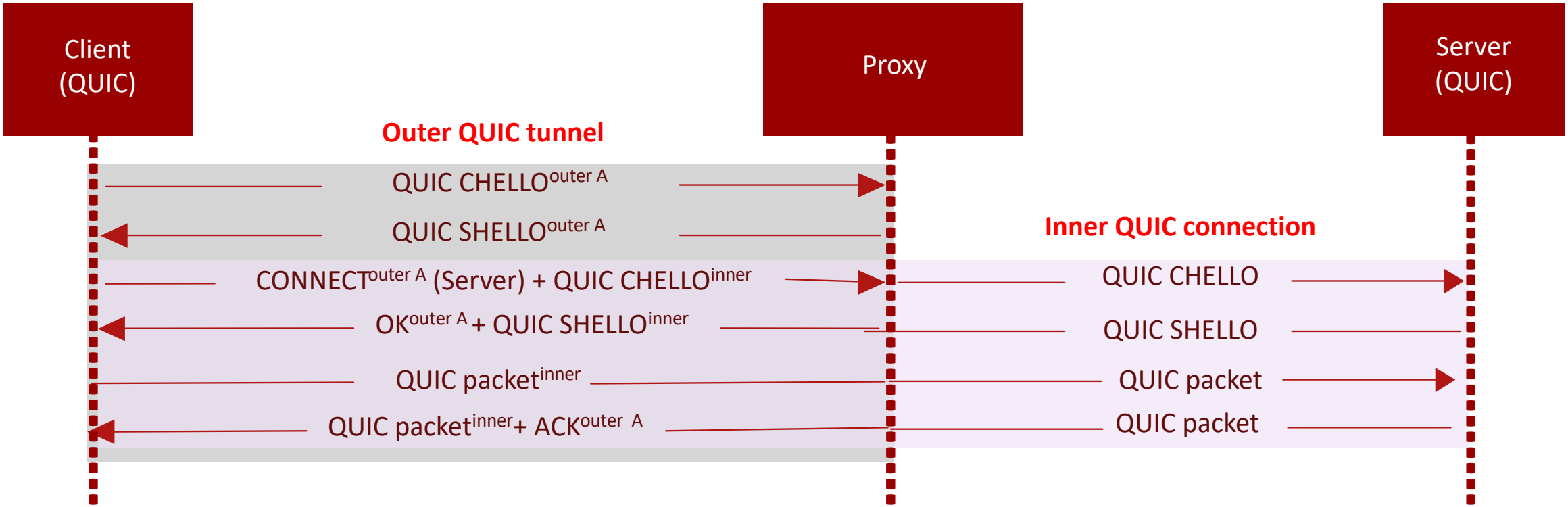
- Make network support functions collaborative and explicit
  - Client and/or server selects proxy and function
  - Tunnelling and encryption protects information exchanged with a proxy from other network interference

Approach



- Client explicitly opens QUIC tunnel connection to proxy
  - use of HTTP CONNECT and MASQUE for forwarding, authentication, and configuration
- QUIC proxy provides secure forwarding and performance enhancement services
  - e.g. congestion control support (mobile/satellite), access policy enforcement, load balancing/mobility, multi-hop chaining/onion routing
- QUIC proxy may optionally also open a tunnel to server (if supported by server)

Connection Establishment



Usage Scenarios
draft-kuehlewind-quic-substrate

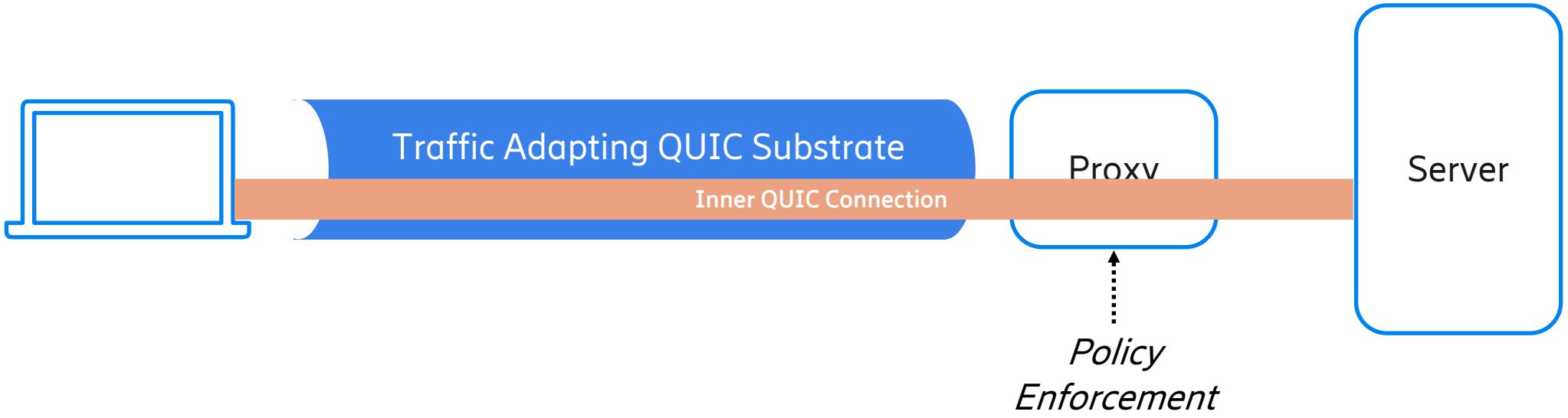
- Obfuscation via Tunneling
- Advanced Support of User Agents
  - Security and Access Policy Enforcement
- Frontend Support for Load Balancing and Migration/Mobility
  - IoT Gateway
- Multi-hop Chaining (aka Onion Routing)

Obfuscation via Tunneling

- Client knows proxy and connects to request forwarding
  - Client and proxy have a trust relationship and can optionally authenticate each other (see MASQUE)
- Server is not aware of the proxy and does not see the clients IP address

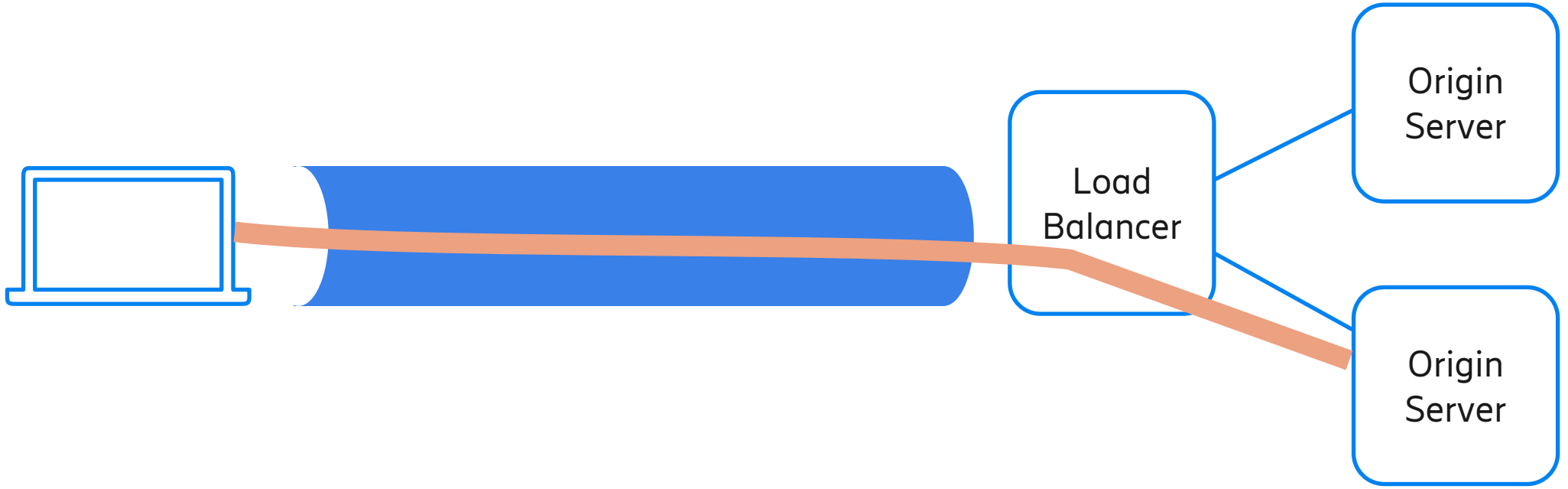
Advanced Support of User Agents

- Proxy provides additional functionality (located "close" to the client e.g. access network)
- Clients request function and may provide information to the proxy; optionally server can be aware



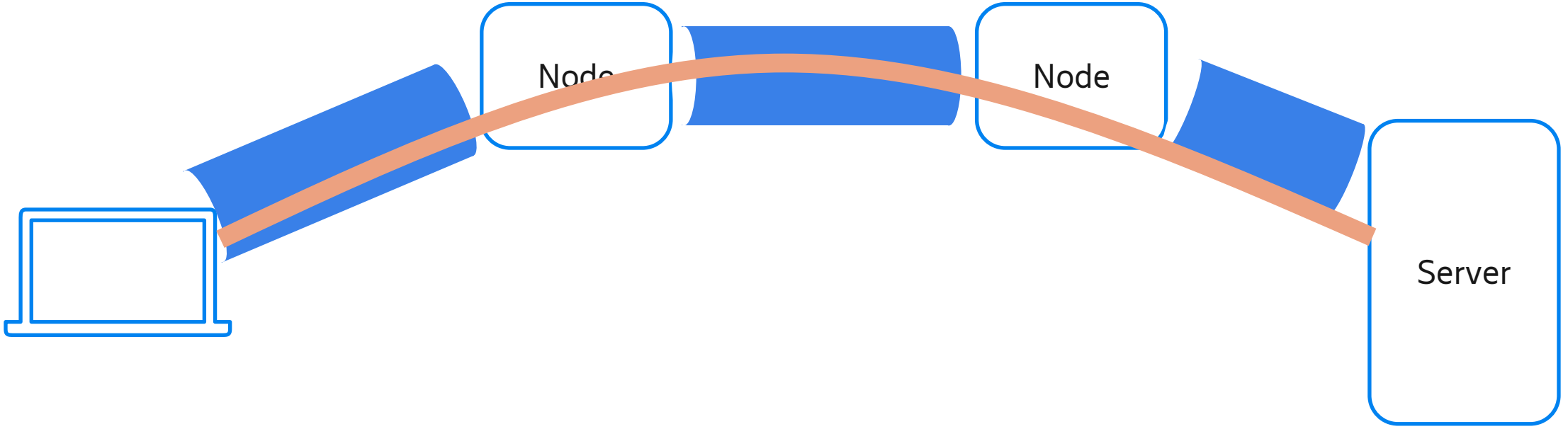
Frontend Support for Load Balancing and Migration/Mobility

- (Reverse) proxy may or may not be under the the same administrative domain as the service provider
- Proxy supports load balancing and/or mobility without terminating the e2e/app security association
- **IoT Gateways**



Multi-hop Chaining (aka Onion Routing)

— Multiple layers of QUIC tunnels can each point to another proxy, enabling TOR-like security



Requirements and Open Issues

— Trust and authentication
— Control protocol and support functions
— Discovery

Drafts

- QUIC as a Substrate - https://tools.ietf.org/html/draft-kuehlewind-quic-substrate-00
- MASQUE - https://tools.ietf.org/html/draft-schinazi-masque
- HTTP Transport Authentication - https://tools.ietf.org/html/draft-schinazi-httpbis-transport-auth-00

- Also, previous and related drafts:
  - HELLIUM - https://tools.ietf.org/html/draft-schwartz-httpbis-helium
  - HINT - https://tools.ietf.org/html/draft-pardue-httpbis-http-network-tunnelling
  - QUIC Datagram - https://tools.ietf.org/html/draft-pauly-quic-datagram