QUIC-LB

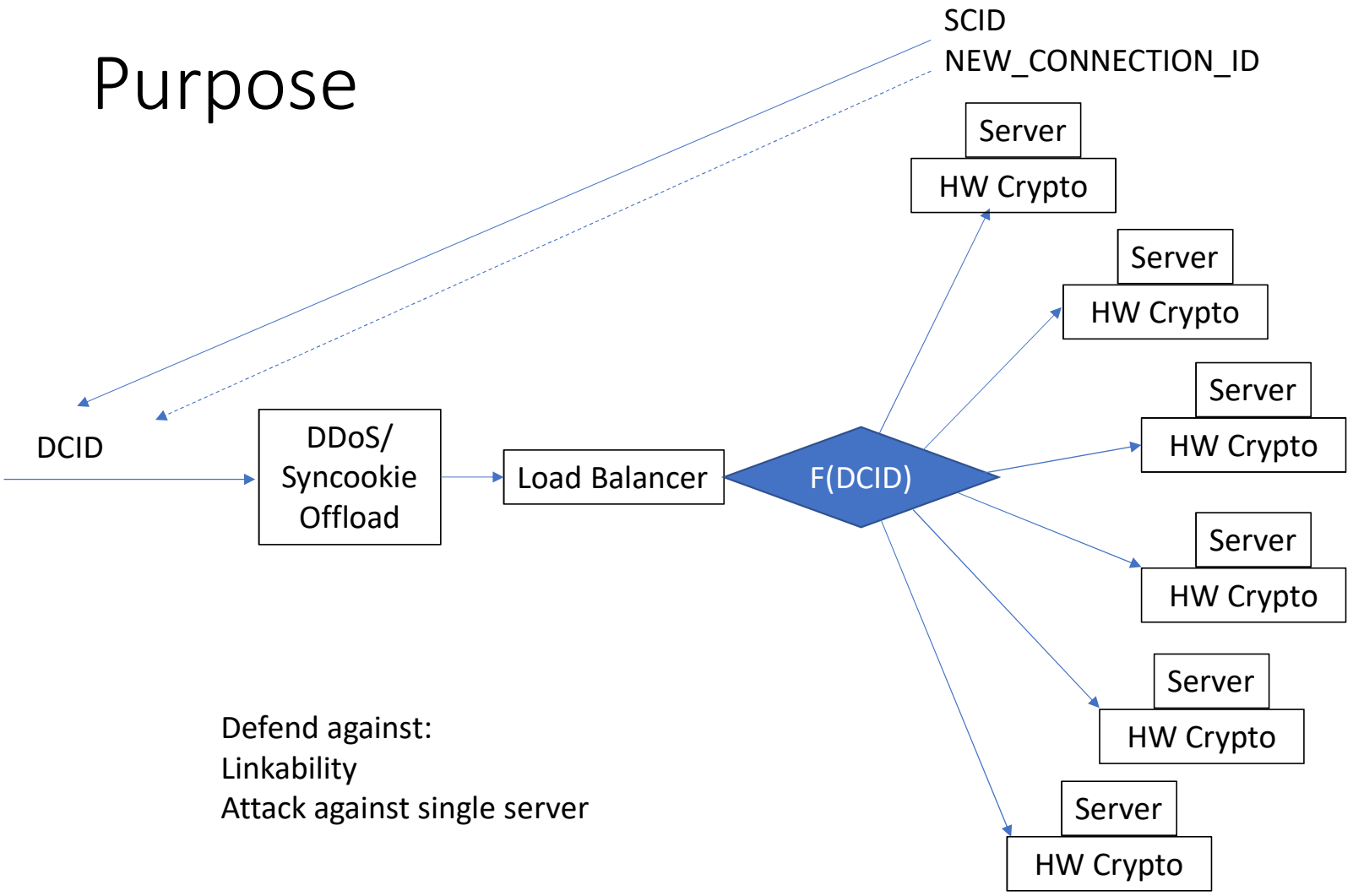
draft-duke-quic-load-balancers-05

Martin Duke

F5 Networks

Interim Meeting, Cupertino, CA, 17 Oct 2019

Purpose



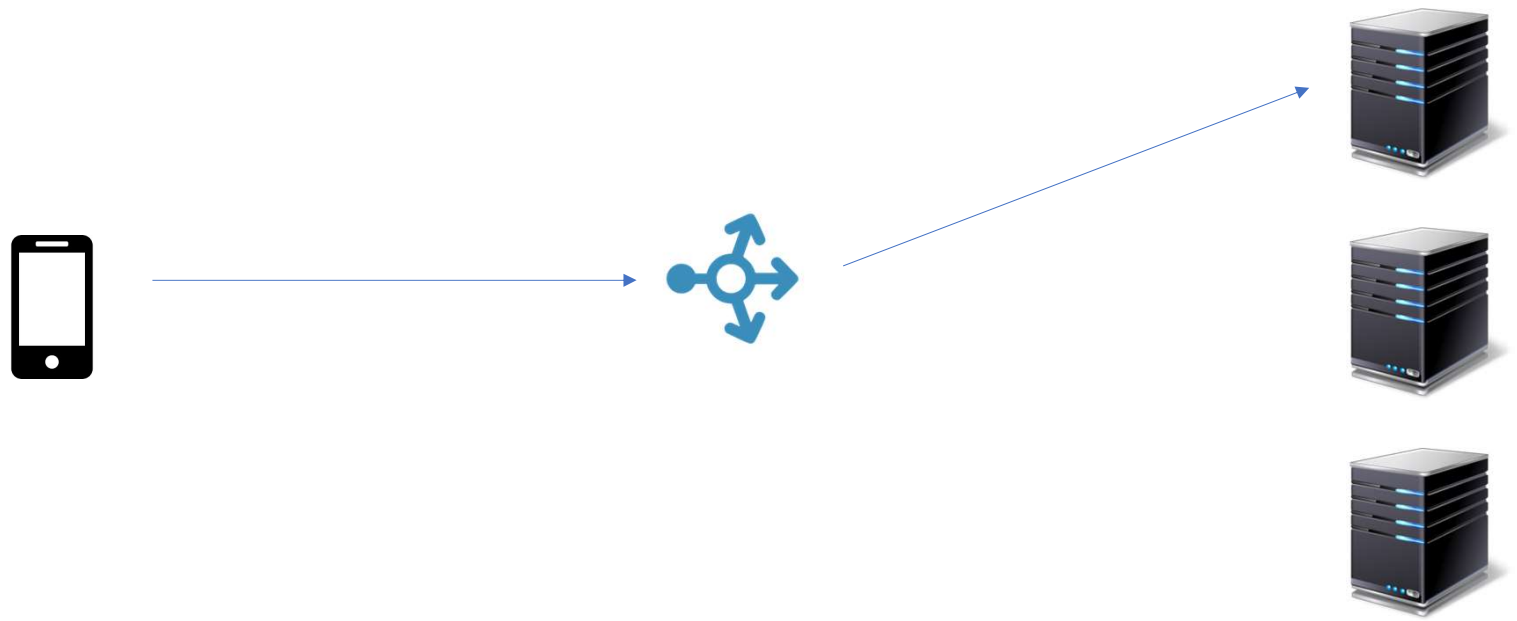
Defend against:
Linkability
Attack against single server

Changes…

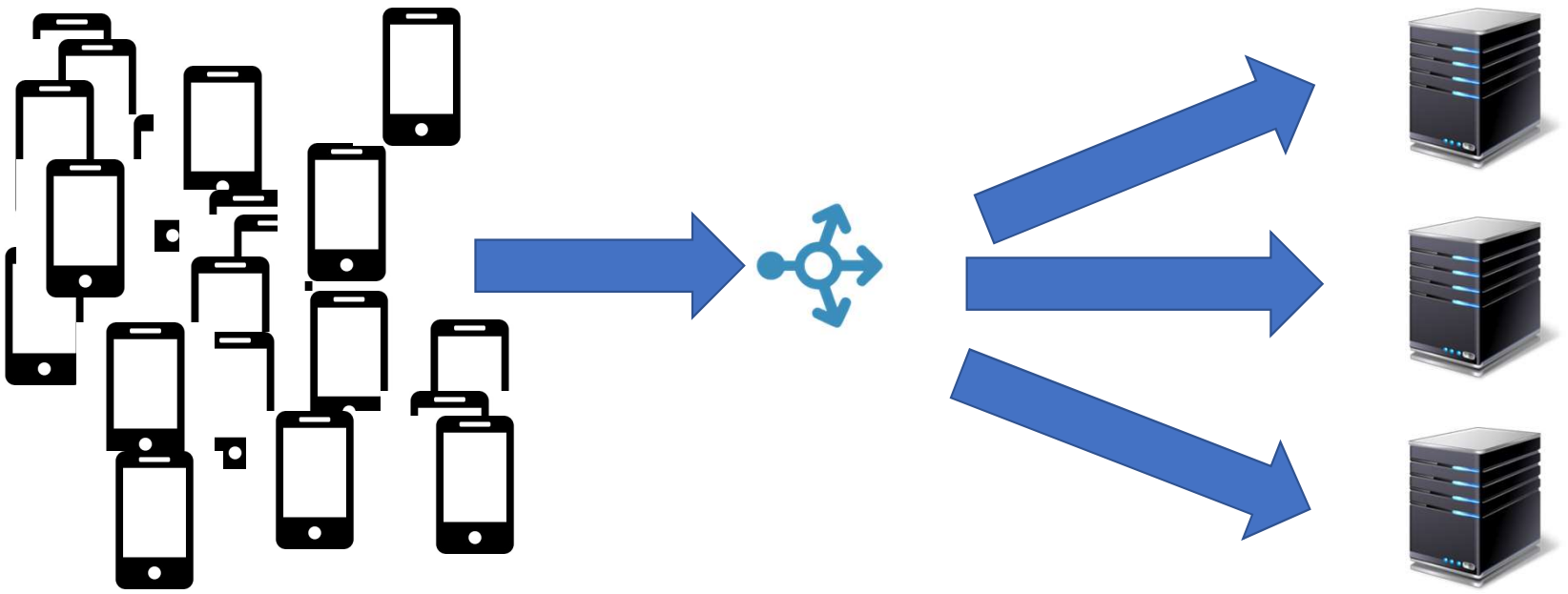
"QUIC tolerates no mediation by L7 middleboxes"

"QUIC tolerates mediation by *explicitly trusted* L7 middleboxes"

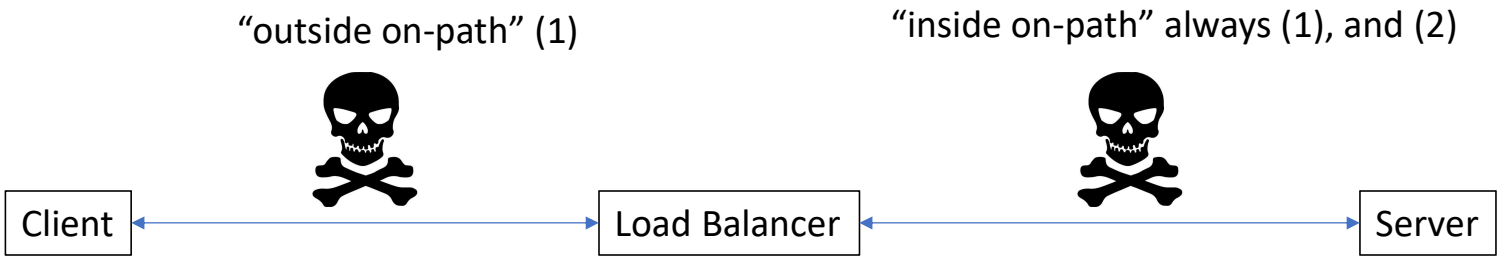
Perfect Linkability



Perfect Unlinkability



Security



“outside off-path” (none)

“inside off-path” (2)

Attacks:
(1) Obtain server mapping
(2) Break LB routing

Configuration Schema

```
UINT2      config_id
BOOL       self-describing length
Switch (retry_service)
           none: N/A
           no-shared-state: N/A
           shared_state: key
Switch (server_encoding_method)
           plaintext: server_id_length, server_id
           obfuscated: routing_mask, divisor, modulus
           stream_cipher: key, server_id_len, server_id
           block_cipher: key, server_id_len, zero_padding_len, server_id
```

Difficult Tradeoffs

- Linkability decisions are made by the server but affect the client.
- When linkability is likely, should servers send disable_active_migration or do best-effort?
- Robustly private methods are costly to implement – might we break NAT robustness and migration entirely if no one implements QUIC-LB?

Next Steps

- Move for adoption in Singapore (?)
- Start interop of algorithms
- Make some tradeoffs