QUIC-LB

draft-duke-quic-load-balancers-02 (already obsolete)

Martin Duke
F5 Networks
IETF 103, 6 Nov 2018
Purpose

Defend against:
Linkability
Attack against single server
Objectives

• Simplicity
• Security
• Middleboxes
Security

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

Algorithms:
• Plaintext CID (9-18 bytes)
• 64-bit Cipher (8-18 bytes)
• 128-bit Cipher (16-18 bytes)

Configuration Methods
• All out-of-band
• Global settings out-of-band
• All in-band
Next Steps

• Land draft-03 (next week?) reflection latest iteration of algorithms
• Start interop on algorithms
• Move for adoption in Tokyo (?)
• RETRY offload support