ZeroTrust-FLBench System Architecture

Kubernetes Cluster

Client 1

Client 2

Client 3

Client 4

Client 5

FL Server
(Aggregator)

Pod 1

Pod 2

Pod 3

SEC0: Baseline

SEC1: NetworkPolicy

SEC2: mTLS

SEC3: Both

Network Profiles

NET0 (0ms)

NET2 (50ms)

NET4 (150ms)