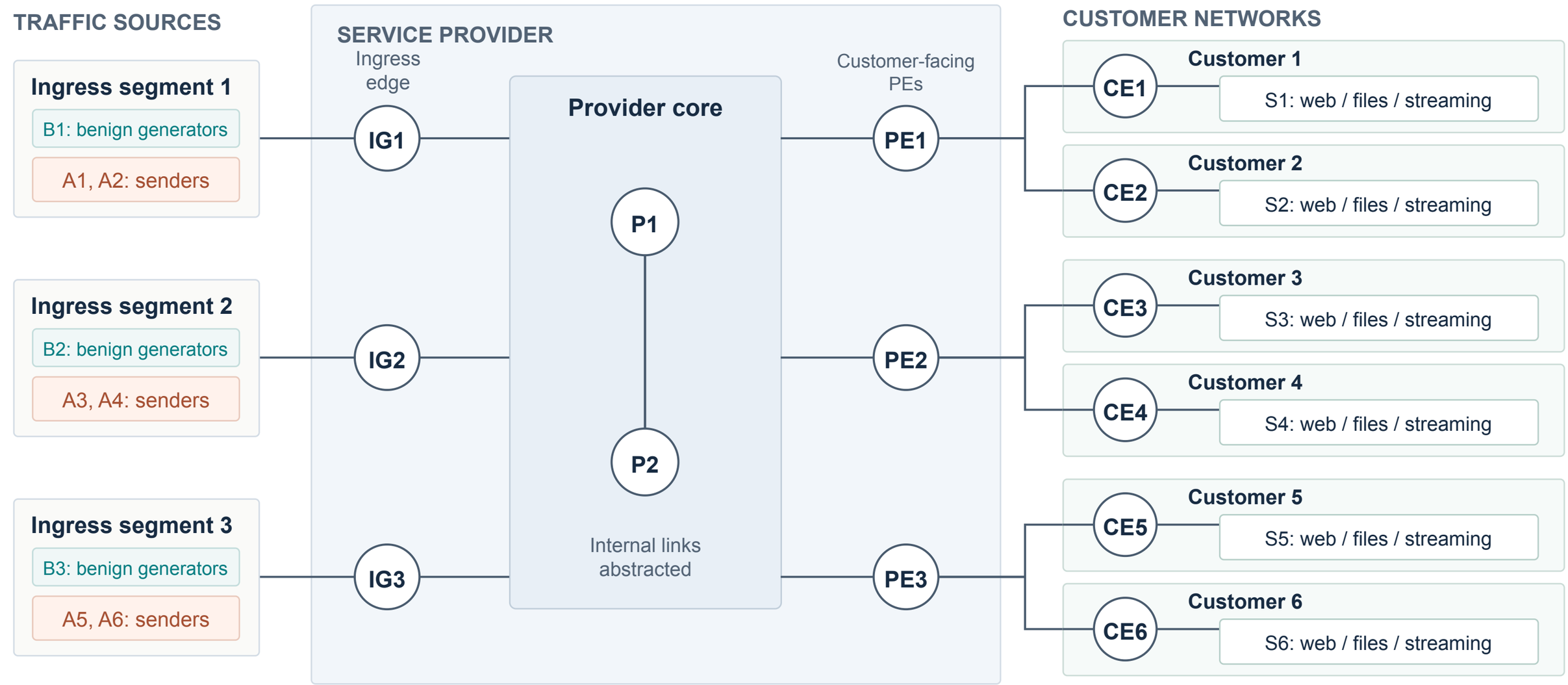
a Proposed service-provider topology

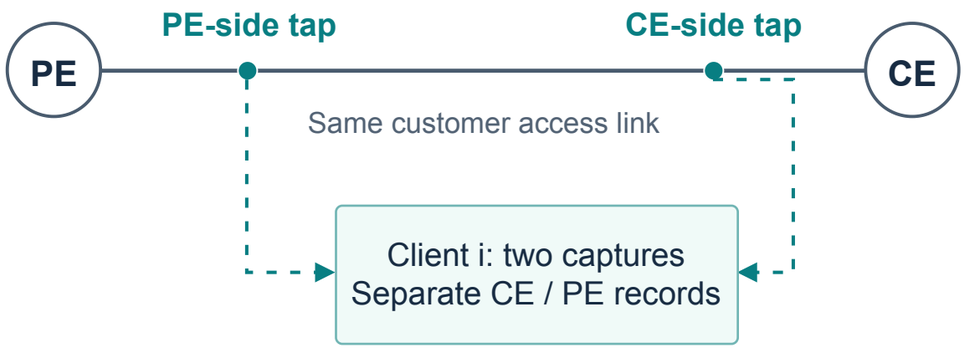
Isolated lab · architecture under development



Six controlled attack senders; three source segments

Linux / FRR routing · services behind every CE

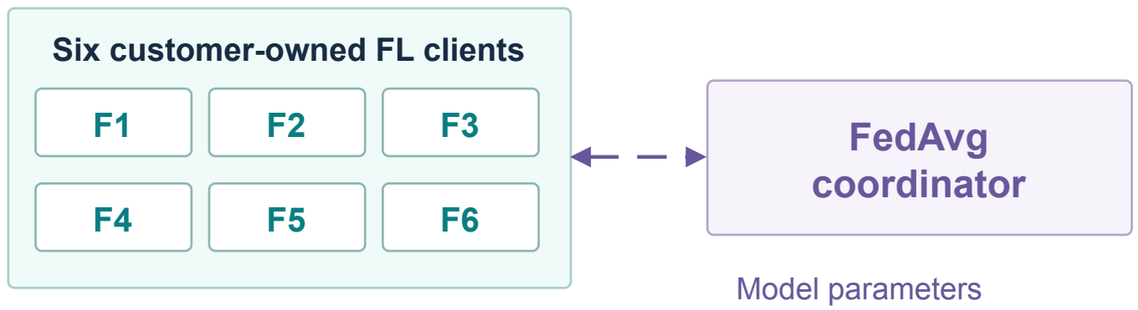
b Paired capture for customer i



One episode · both directions · receive-only mirrors

Compare one view at a time with equal compute resources

c Federated learning on management network



Management traffic stays outside data-plane captures

Local training: SGD / Adam; QiML implementation pending

Bidirectional data path

Passive packet copy

Model updates / global model