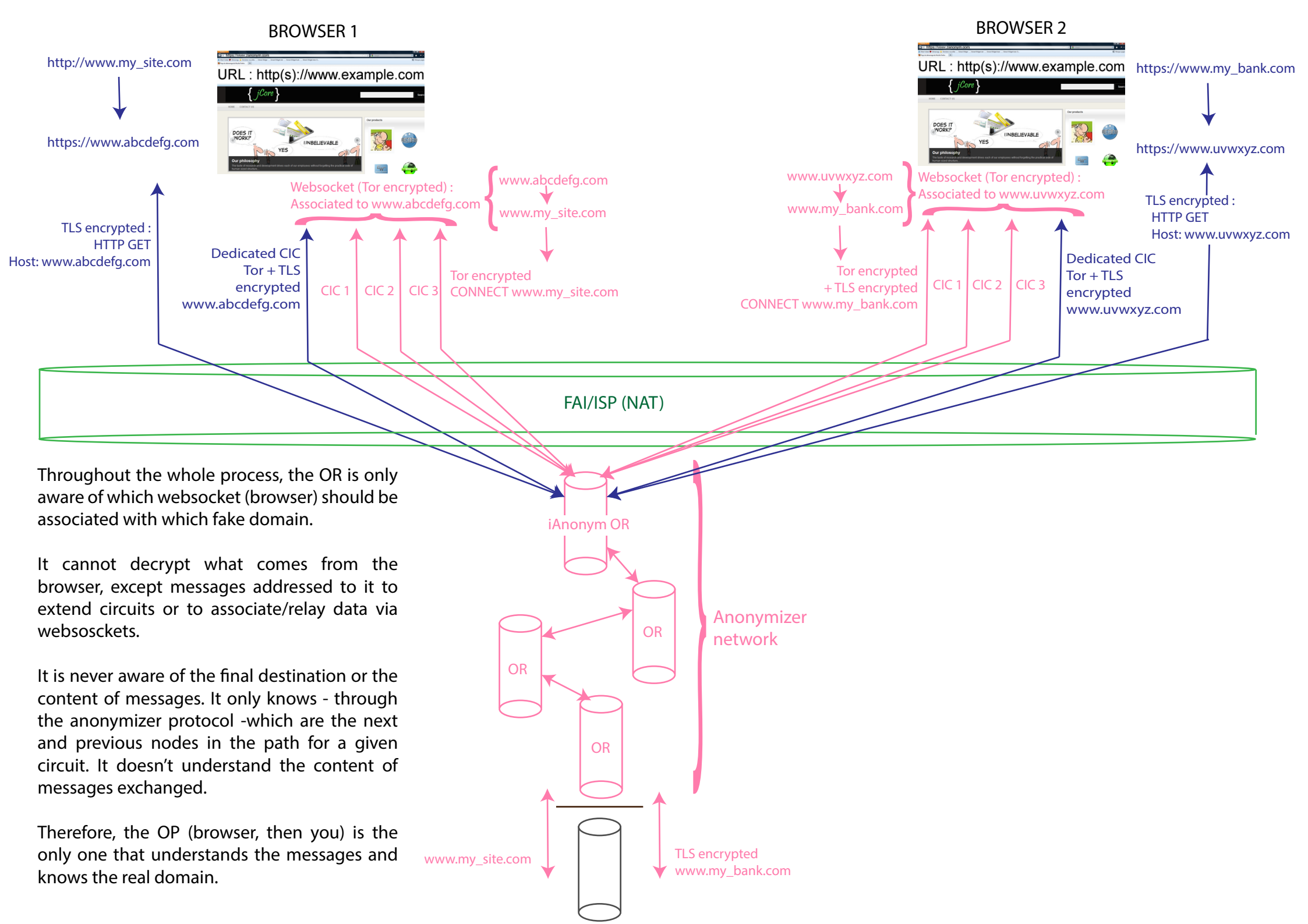

Throughout the whole process, the OR is only aware of which websocket (browser) should be associated with which fake domain.

It cannot decrypt what comes from the browser, except messages addressed to it to extend circuits or to associate/relay data via websosckets.

It is never aware of the final destination or the content of messages. It only knows - through the anonymizer protocol -which are the next and previous nodes in the path for a given circuit. It doesn't understand the content of messages exchanged.

Therefore, the OP (browser, then you) is the only one that understands the messages and knows the real domain.