

BROWSER 1

http://www.my_site.com
↓
https://www.abcdefg.com



Websocket (Tor encrypted) :
Associated to www.abcdefg.com

www.abcdefg.com
↓
www.my_site.com

Tor encrypted
CONNECT www.my_site.com

CIC 1
CIC 2
CIC 3

Dedicated CIC
Tor + TLS
encrypted
www.abcdefg.com

TLS encrypted :
HTTP GET
Host: www.abcdefg.com

BROWSER 2



Websocket (Tor encrypted) :
Associated to www.uvwxyz.com

www.uvwxyz.com
↓
www.my_bank.com

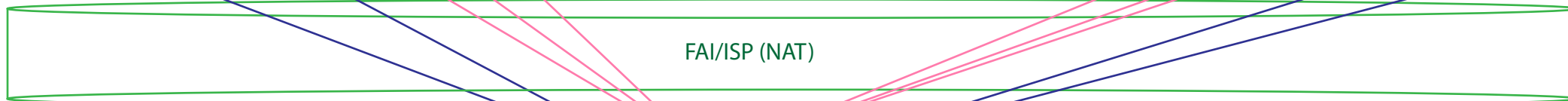
Tor encrypted
+ TLS encrypted
CONNECT www.my_bank.com

CIC 1
CIC 2
CIC 3

Dedicated CIC
Tor + TLS
encrypted
www.uvwxyz.com

https://www.my_bank.com
↓
https://www.uvwxyz.com

TLS encrypted :
HTTP GET
Host: www.uvwxyz.com



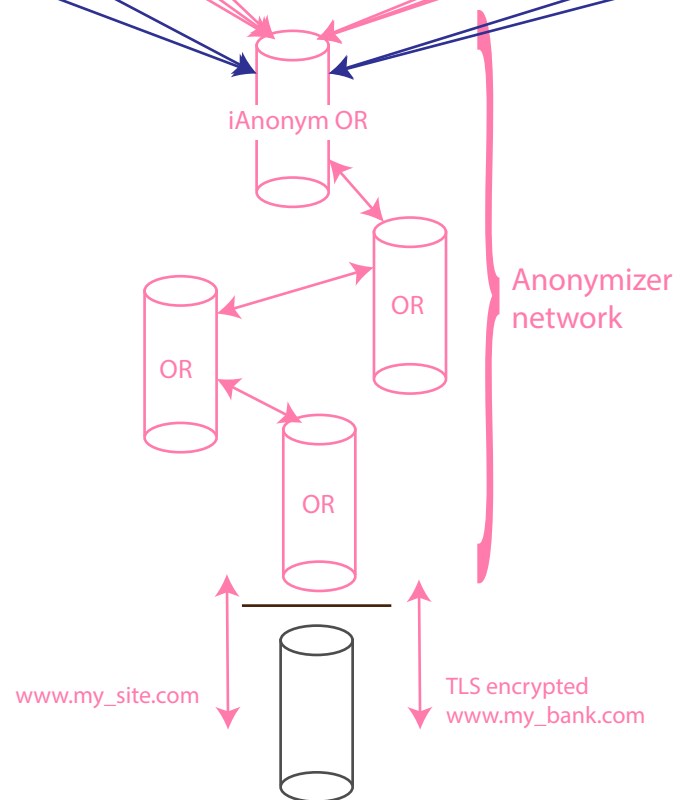
FAI/ISP (NAT)

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 websockets.

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.



iAnonym OR

Anonymizer
network

OR

OR

OR

OR

www.my_site.com

TLS encrypted
www.my_bank.com