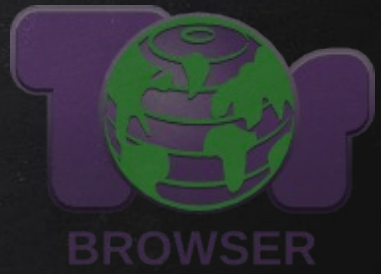
TOR-Browser

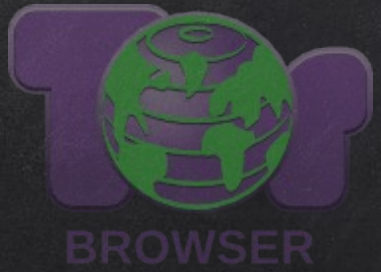


- Modified version of Firefox ESR.
- Uses the TOR network by default.
- Disables insecure features/plugins .
- Disables features/plugins that could deanonymize you.
- Forces all connections over HTTPS (using https-everywhere plugin).
- Disables scripts (using noscript plugin).

Note:

With TOR Browser only traffic sent via the browser is routed through the TOR network.

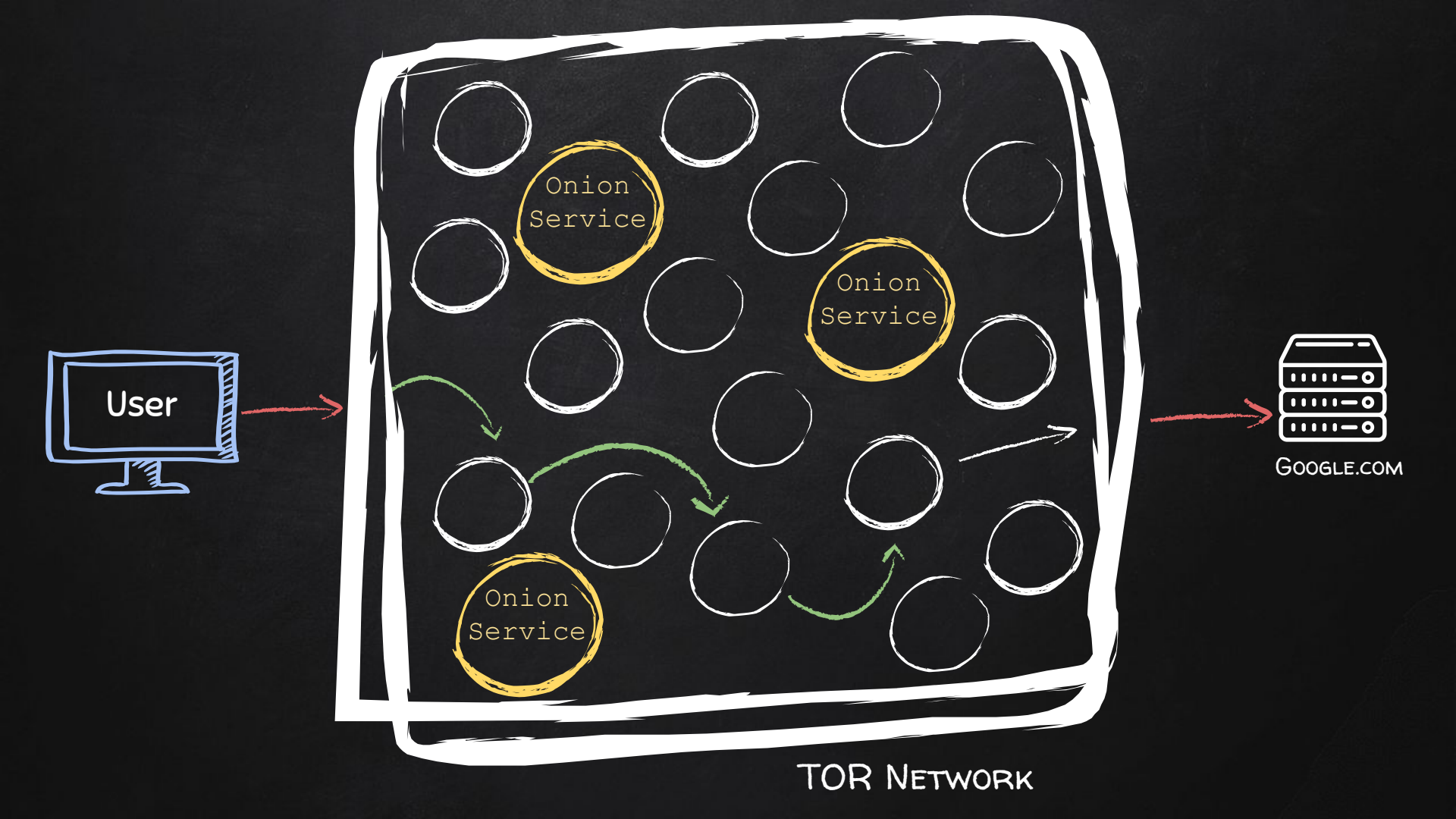
TOR-Browser



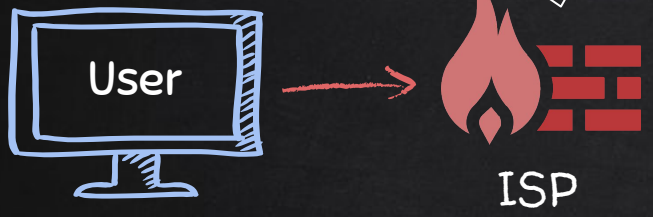
- Modified version of Firefox ESR.
- Uses the TOR network by default.
- Disables insecure features/plugins .
- Disables features/plugins that could deanonymize you.
- Forces all connections over HTTPS (using https-everywhere plugin).
- Disables scripts (using noscript plugin).

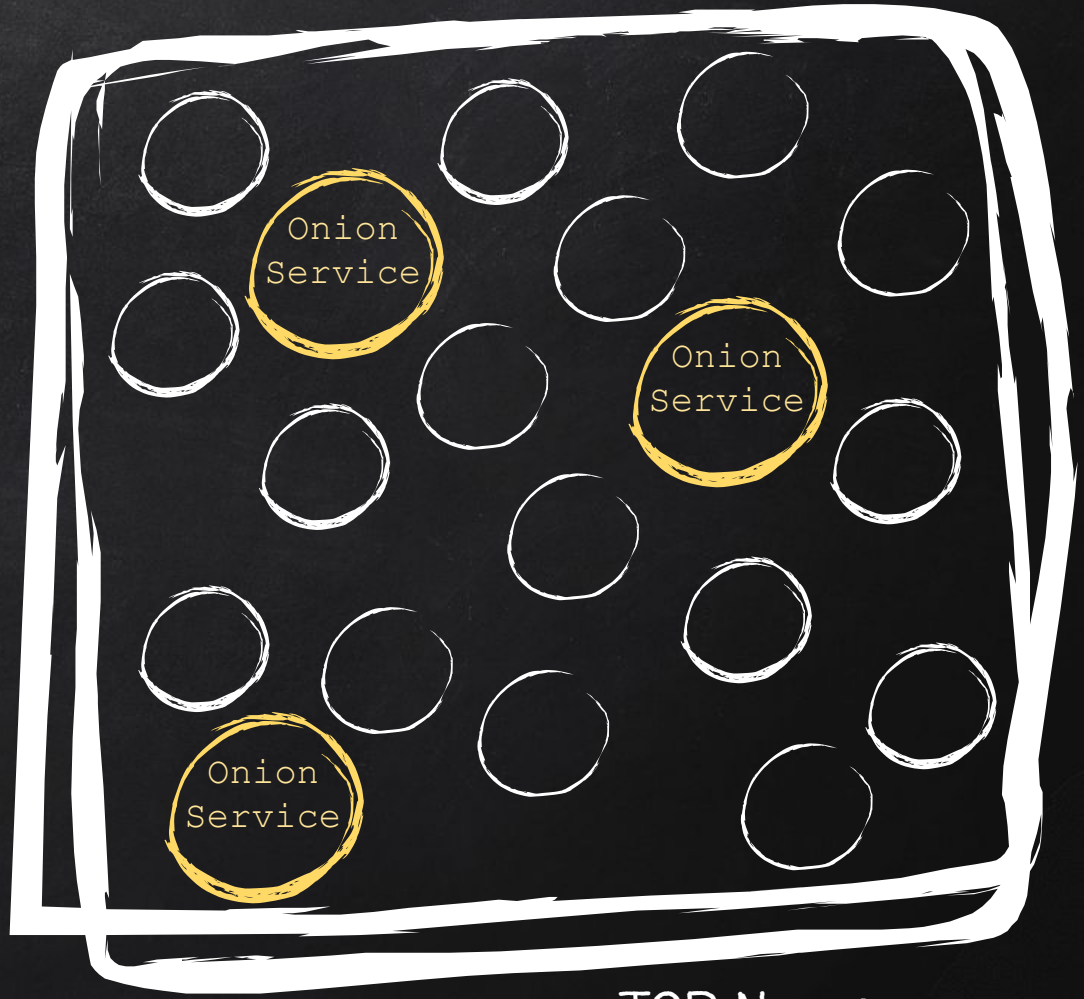
Note:

With TOR Browser only traffic sent via the browser is routed through the TOR network.


User
Onion Service
Onion Service
Onion Service
Google.com
TOR Network

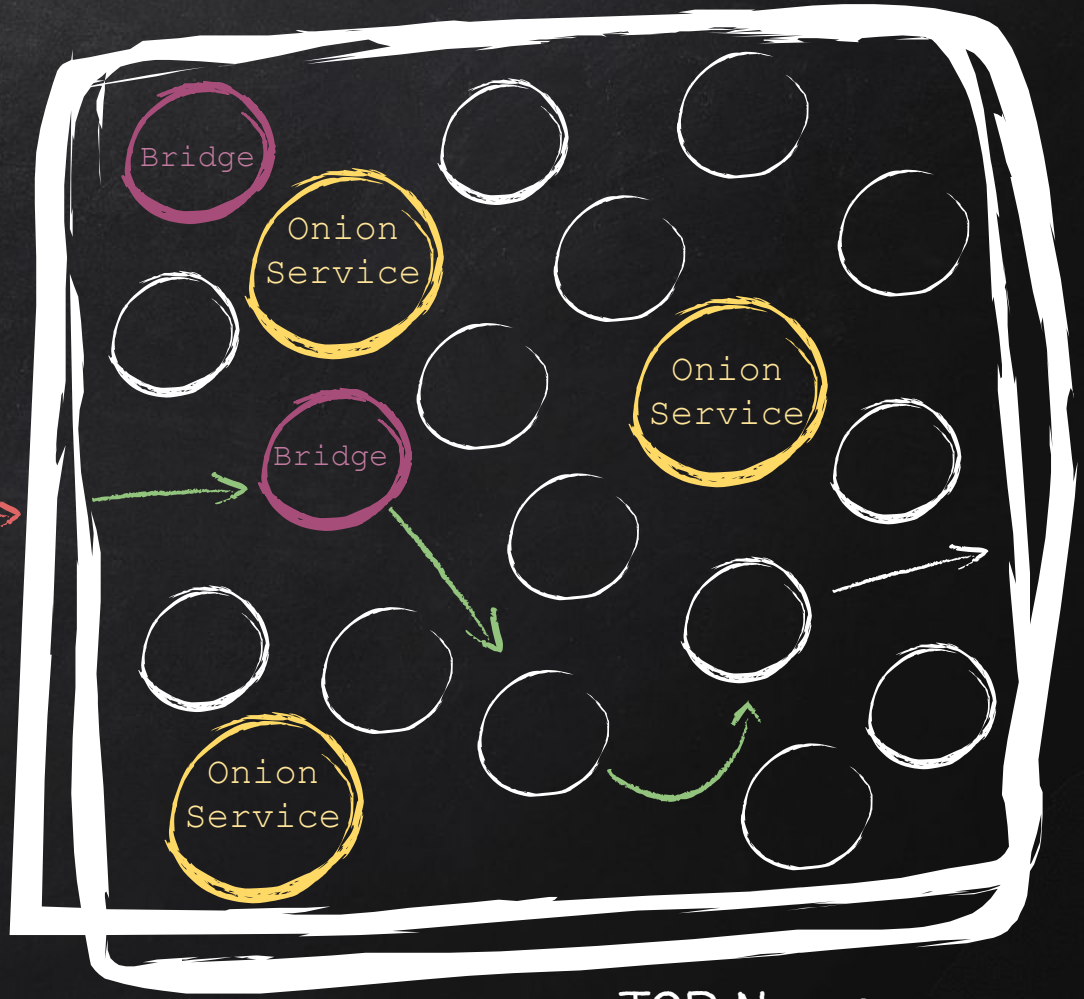
1. Block ALL tor relays.





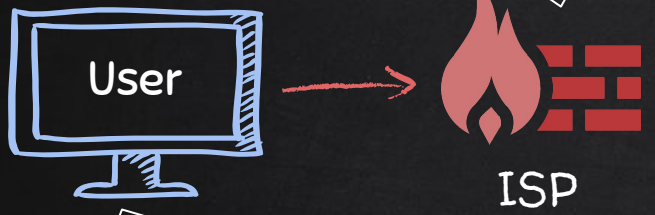
1. Block ALL tor relays.

1. Use unpublished relays (bridges).

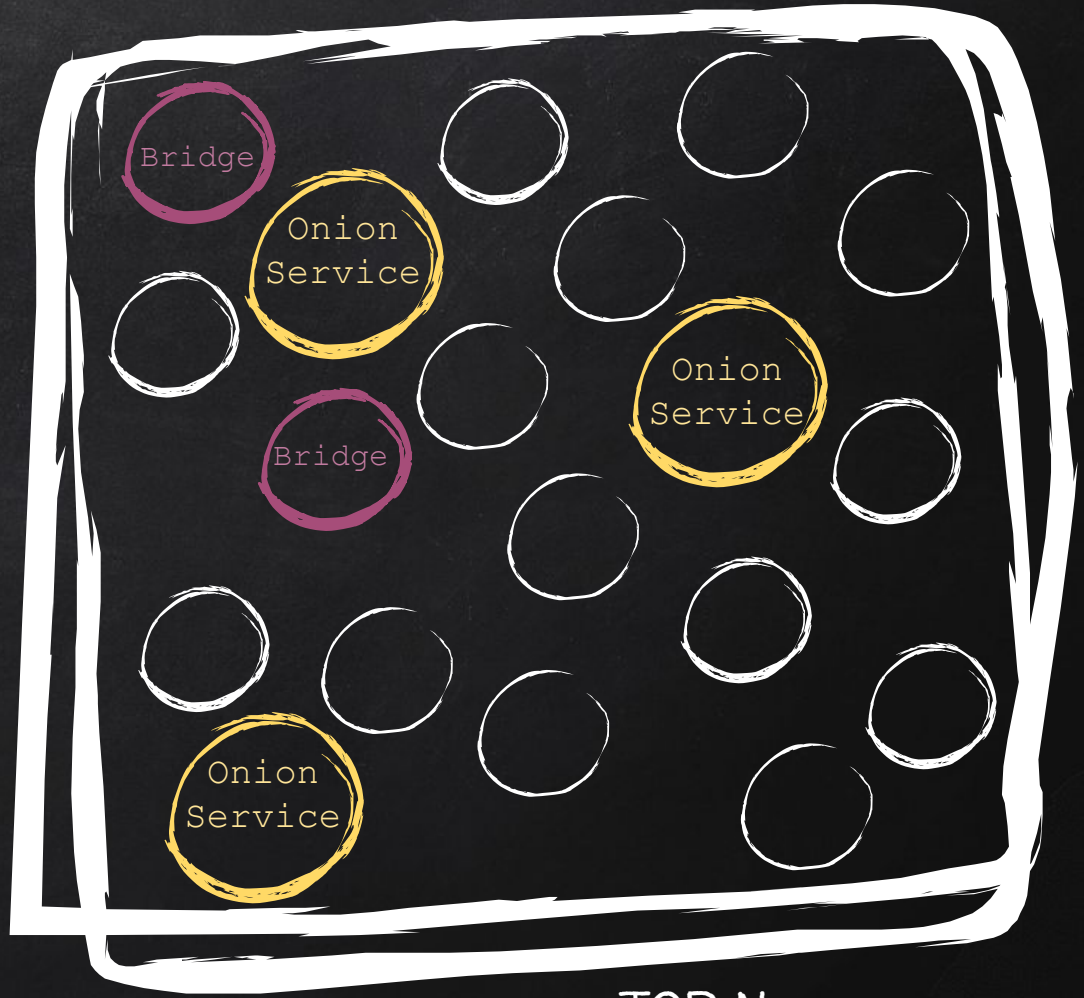


1. Block ALL tor relays.

2. Use DPI (Deep Packet Filtering) to identify and block TOR traffic.

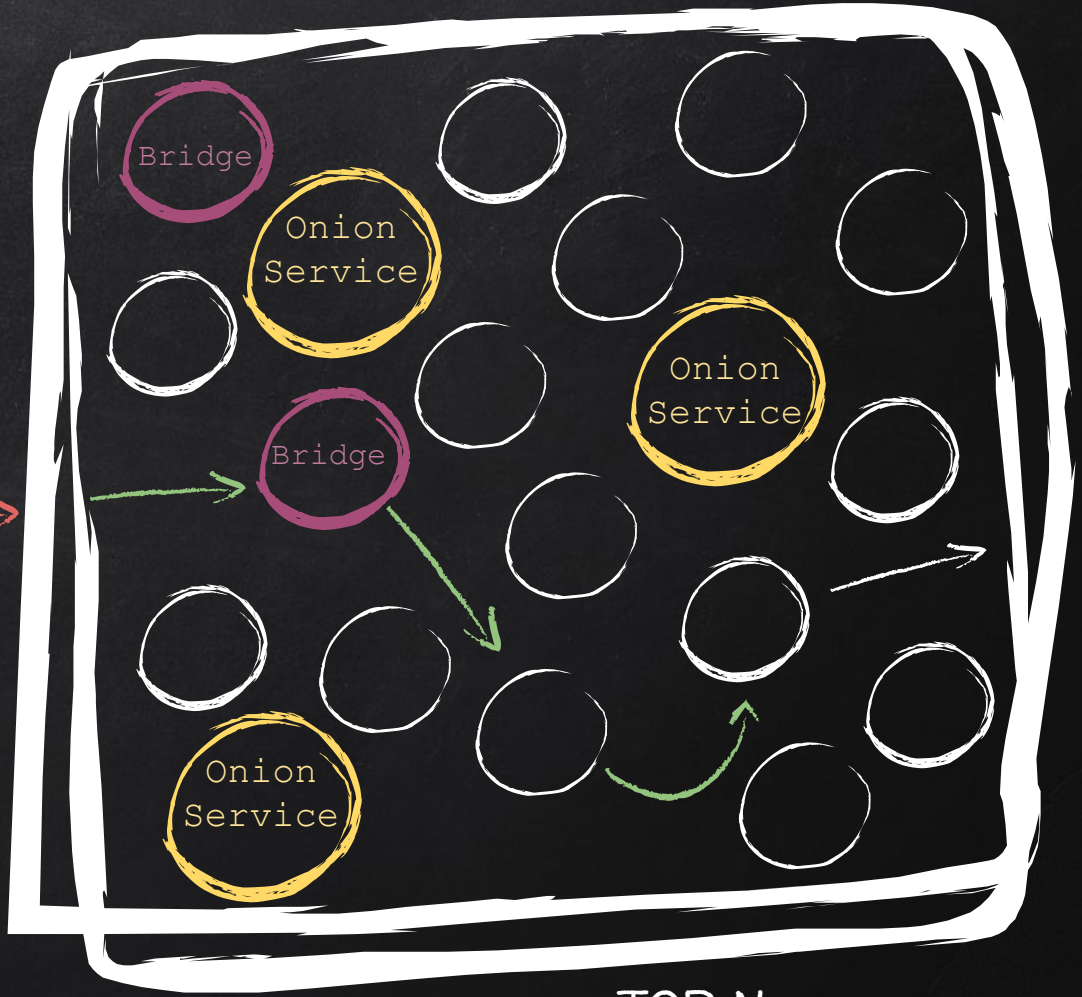


1. Use unpublished relays (bridges).



1. Block ALL tor relays.
2. Use DPI (Deep Packet Filtering) to identify and block TOR traffic.

1. Use unpublished relays (bridges).
2. Use pluggable transports to obfuscate traffic.

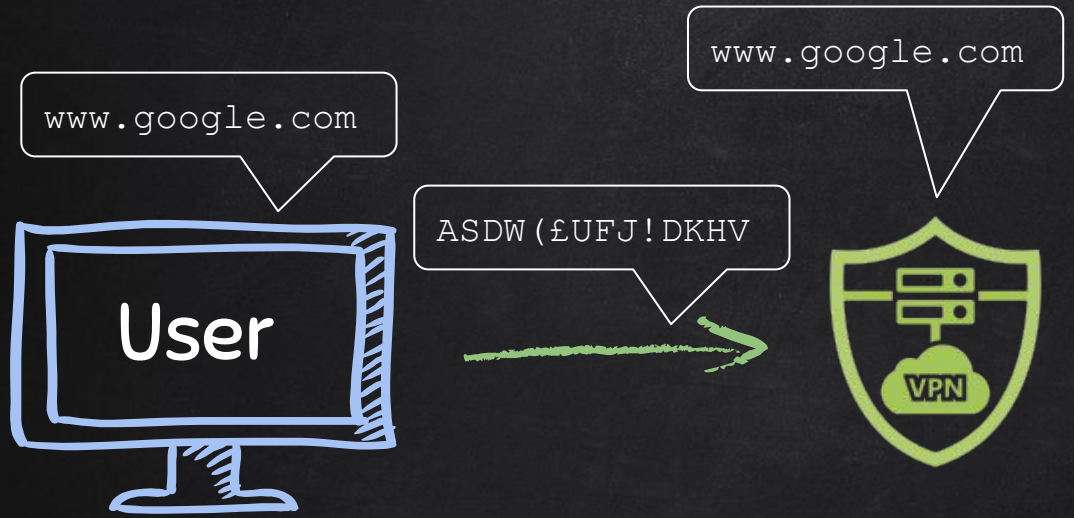


VPN – Virtual Private Network

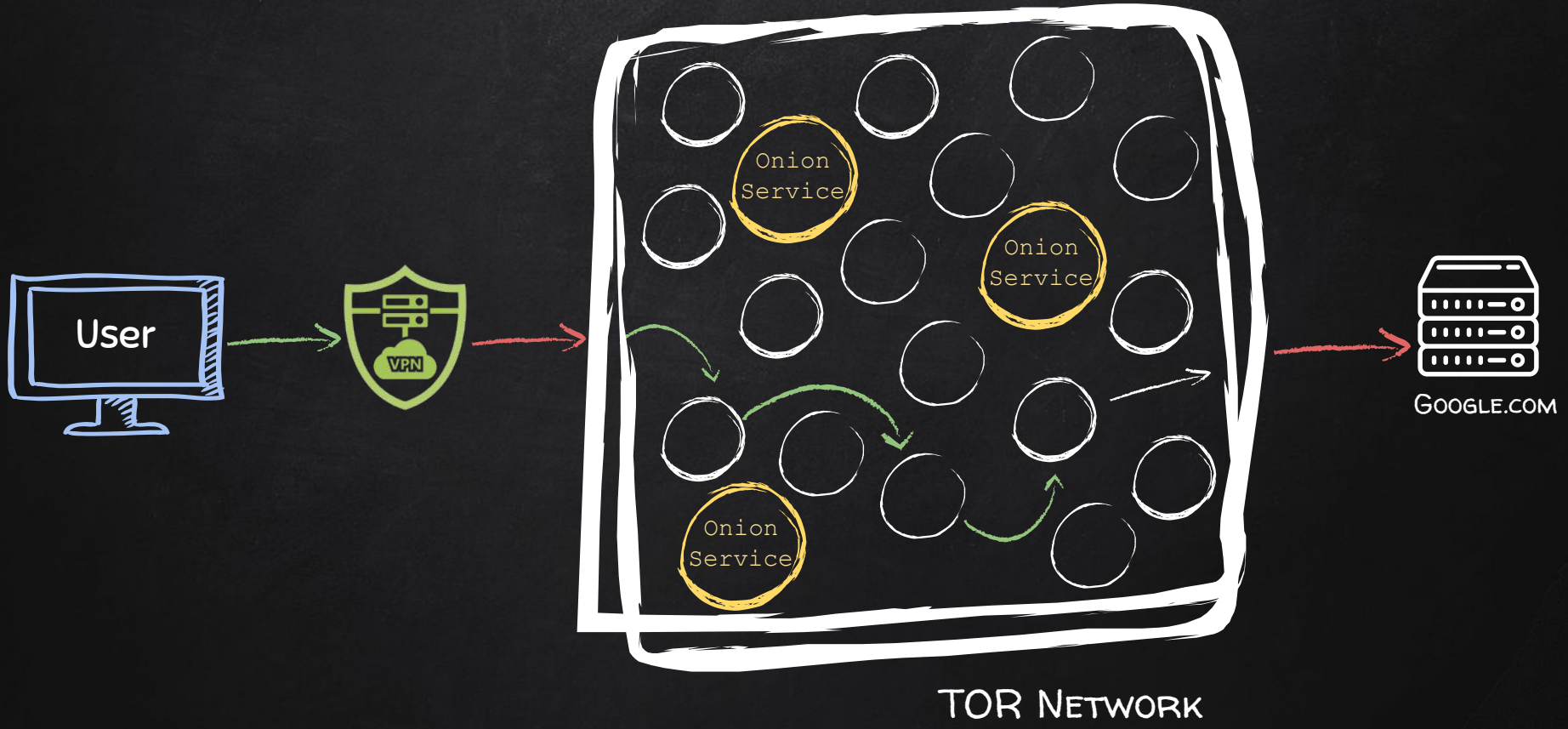

User
Google.com


User
VPN

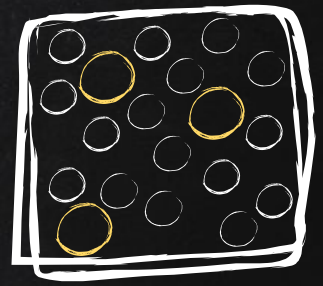

www.google.com
User
www.google.com
VPN


www.google.com
User
ASDW(£UFJ!DKHV
www.google.com
VPN


www.google.com
User
ASDW(£UFJ!DKHV
www.google.com
VPN
Google.com


User
VPN
Onion Service
Onion Service
Onion Service
Google.com
TOR Network

TOR Network



Internet

Benefits:

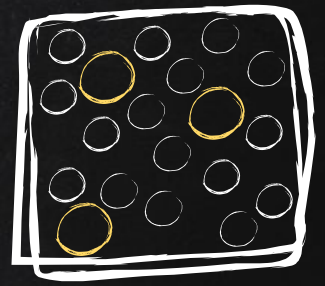
- Extra layer of encryption.
- More privacy & anonymity.
- Bypass censorship.


User
ISP
VPN
Onion Service
Onion Service
Onion Service
TOR Network

Worst Case Scenario

Pluggable transports & Bridges	VPN
Connecting to TOR	Connecting to a VPN.

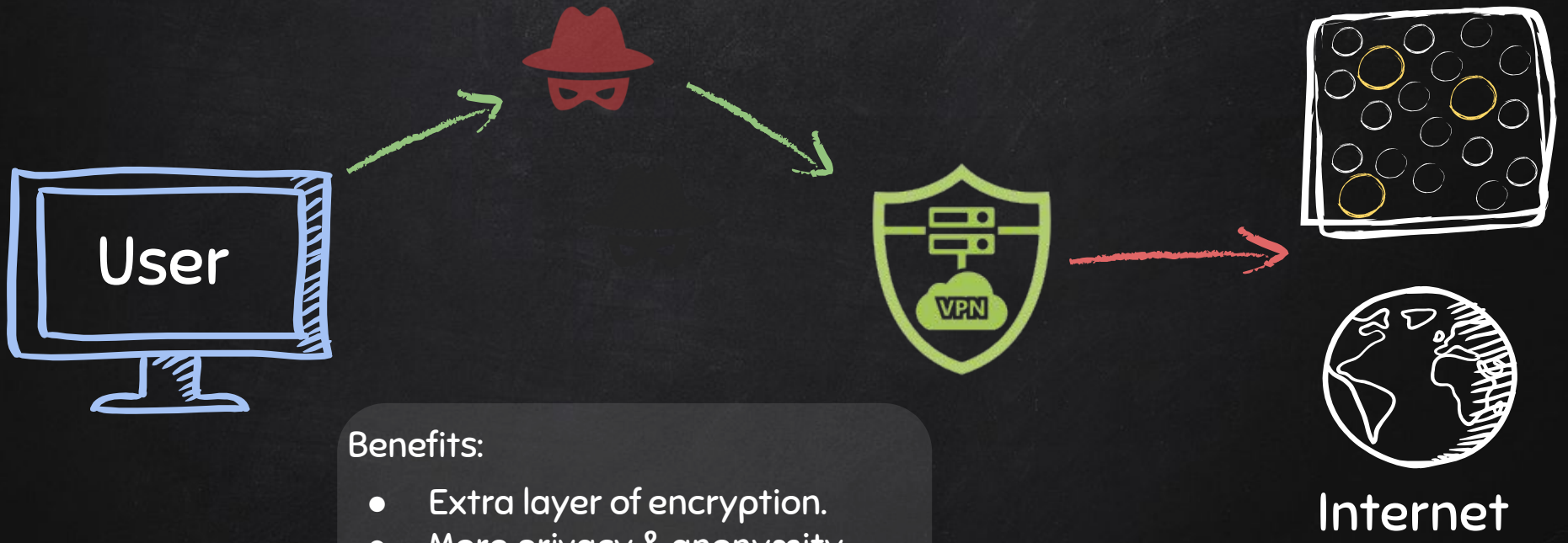
TOR Network



Internet

Benefits:

- Extra layer of encryption.
- More privacy & anonymity.
- Bypass censorship.
- Protection from hackers.



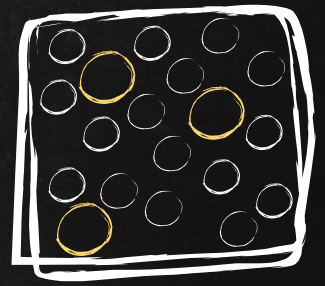
Benefits:

- Extra layer of encryption.
- More privacy & anonymity.
- Bypass censorship.
- Protection from hackers.

Notes:

- Use reputable VPN.

TOR Network



Internet

Notes:

- Use reputable VPN.
- Avoid free providers.

Notes:

- Use reputable VPN.
- Avoid free providers.
- Make sure they keep no logs.

Notes:

- Use reputable VPN.
- Avoid free providers.
- Make sure they keep no logs.
- Use HTTPS everywhere.

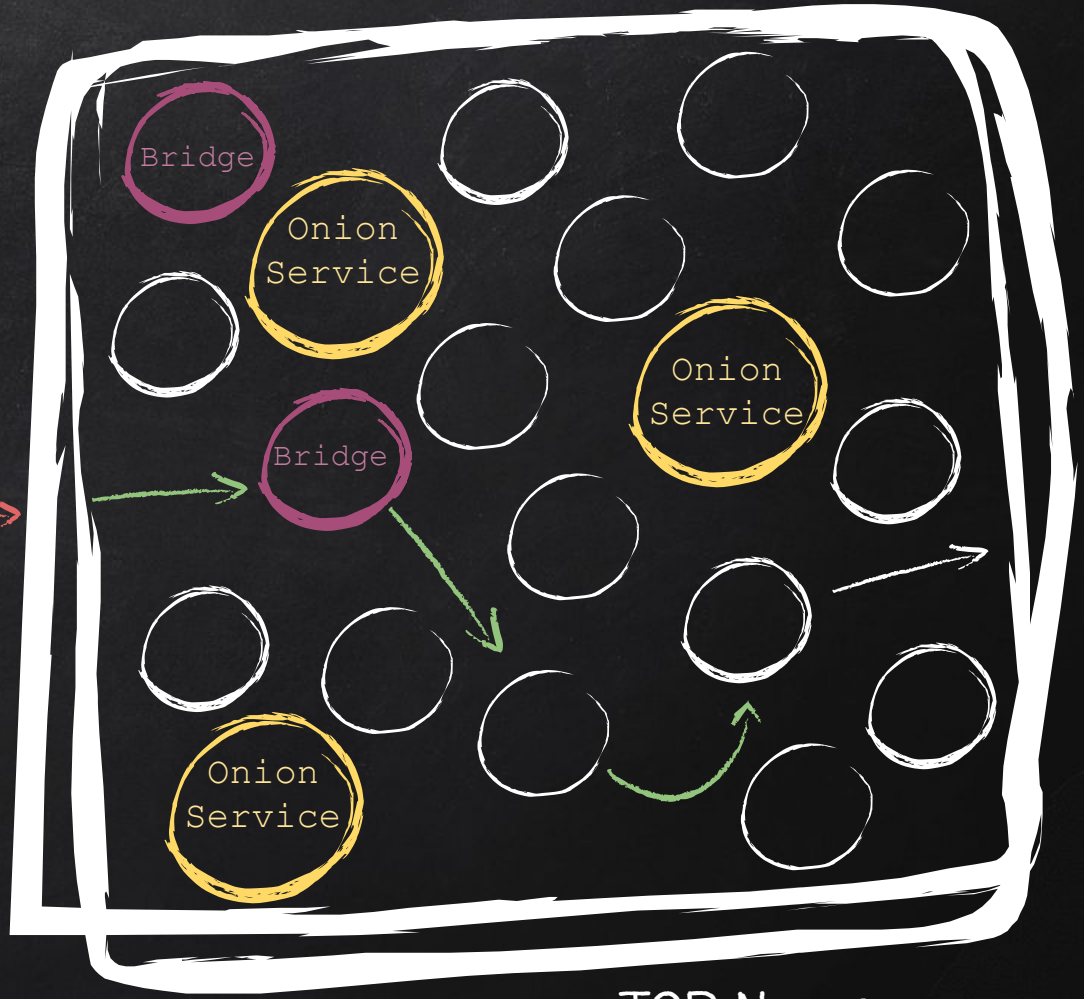
Notes:

- Use reputable VPN.
- Avoid free providers.
- Make sure they keep no logs.
- Use HTTPS everywhere.
- Optional – pay with crypto.


User
VPN
Google.com

1. Block ALL tor relays.

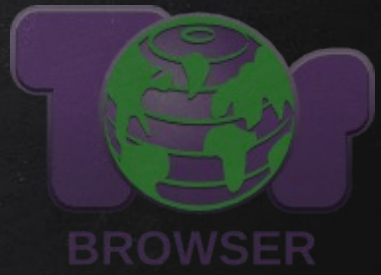
1. Use unpublished relays (bridges).




ISP
User
Internet


ISP
User
Internet

Information Theory



$$\Delta S = - \log_2 Pr(X=x)$$

- The amount of info a fact gives about an entity is measured in bits.
- Entropy (S) measures information in bits.
- ΔS measures how many bits of information the fact X reveals about a target.
- Population of earth at the time of recording this lecture is 7714576923.
- Therefore we need Log2(1 / 7714576923) = 32.8 bits of information to deduce the identity of a person!