

Υπηρεσίες Ονιον

Παραφέστας Νίκος

Ξάνθη, 31 Δεκεμβρίου 2023

Περιεχόμενα

Δίκτυο tor - Γενικά

Υπηρεσίες onion

Πρόσβαση στις υπηρεσίες onion

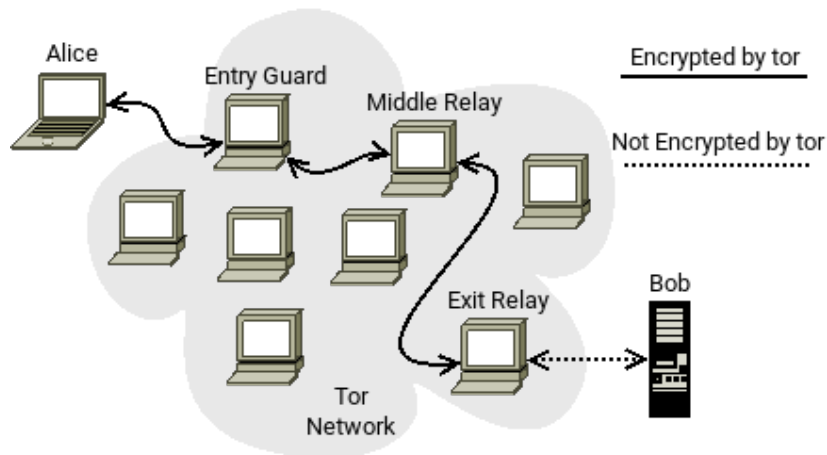
Άδεια χρήσης

Επιθέσεις στις υπηρεσίες onion

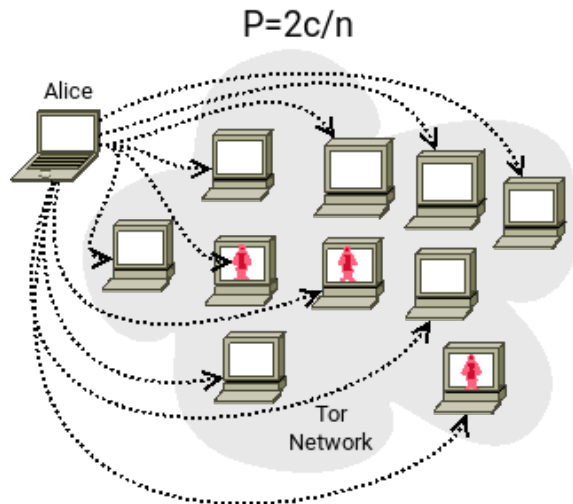
1. Δίκτυο tor

Σύντομη περιγραφή του δικτύου tor

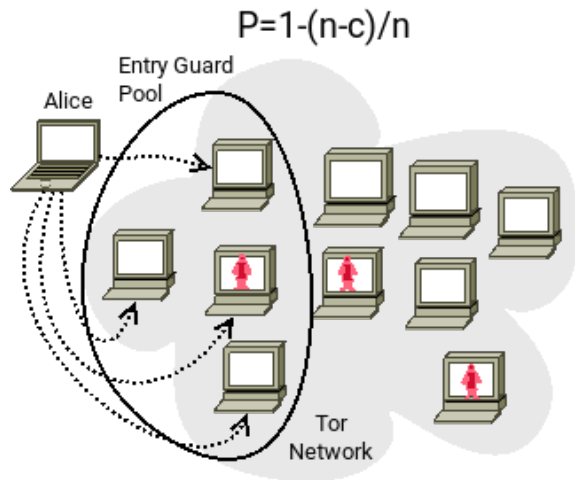
Περιγραφή λειτουργίας δικτύου tor



1. Περιγραφή λειτουργίας δικτύου tor - Entry Guard

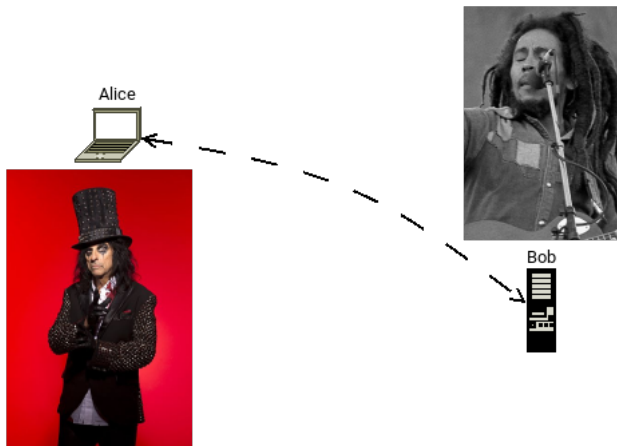


1. Περιγραφή λειτουργίας δικτύου tor - Entry Guard



Συμβατική επικοινωνία μέσω Internet

Δεν υπάρχει ανωνυμία στην επικοινωνία για κανένα μέρος

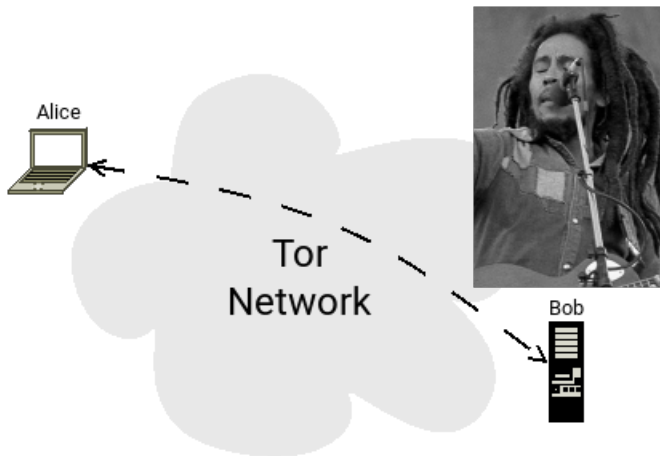


Alice: Πηγή: https://foundation.wikimedia.org/wiki/File:Alice_Cooper_2011.jpg - Άδεια: CC-BY 3.0 Unported

Bob: Πηγή: [https://foundation.wikimedia.org/wiki/File:Bob_Marley_3_\(cropped\).jpg](https://foundation.wikimedia.org/wiki/File:Bob_Marley_3_(cropped).jpg) - Άδεια: CC-BY 2.0 Generic

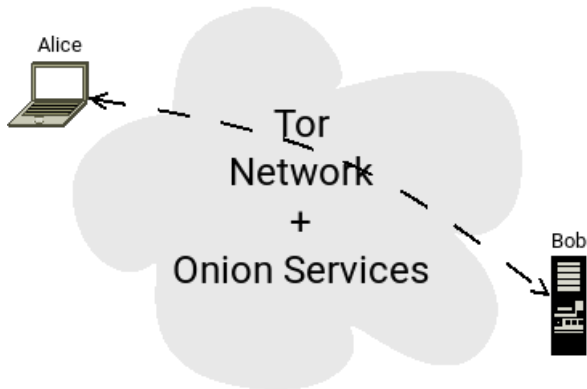
Χρήση tor από τον client

Υπάρχει ανωνυμία από το τον client, αλλά όχι για τον server



Χρήση υπηρεσιών onion

Υπάρχει ανωνυμία και στα δύο μέρη



2. Υπηρεσίες Οnion

Διευθύνσεις υπηρεσιών onion

Η πρόσβαση στις υπηρεσίες onion γίνεται μέσω μία διεύθυνση της μορφής:

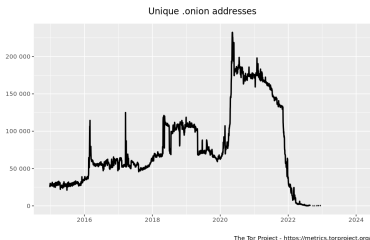
`x5u6sk242wnsohyivyyixzpkcr2szut5aarpyomv2lg6g2qtp5dv4l3qd.onion`

Αποτελείται 56 χαρακτήρες που προκύπτουν από το πλήρες ed25519 ιδιωτικό κλειδί του server. Αυτή είναι η τρέχουσα έκδοση (V3) που συστήνεται από την ομάδα ανάπτυξης του tor.

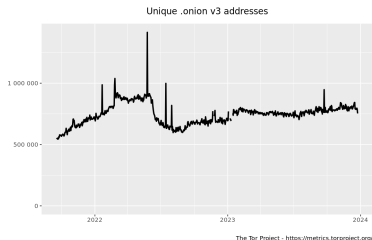
Διευθύνσεις υπηρεσιών onion V2 vs V3

V2: Αποτελείται από 16 χαρακτήρες¹, που προκύπτουν από το SHA1 hash των πρώτων 80 χαρακτήρων του ιδιωτικού κλειδιού του server. Πλέον θεωρείται παρωχημένη και μη ασφαλής.

V2



V3

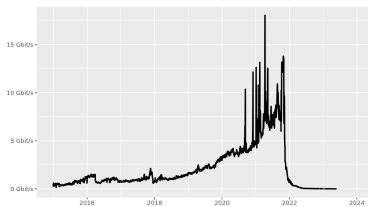


¹π.χ. e3mhbshg7kx5tfyd.onion

Κίνηση Υπηρεσιών Onion

V2

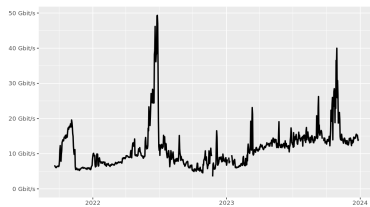
Onion-service traffic



The Tor Project - <https://metrics.torproject.org/>

V3

Onion-service traffic v3



The Tor Project - <https://metrics.torproject.org/>

Πρόσβαση (ενδεικτικά)



Tor Browser



Other Browser



Chat



e-mail clients

Tor Browser trademark: <https://www.torproject.org/about/trademark/>

Mozilla trademark: <https://www.mozilla.org/en-US/foundation/trademarks/policy/>

Icecat & Icedove licence: <https://www.gnu.org/software/gnuzilla/>

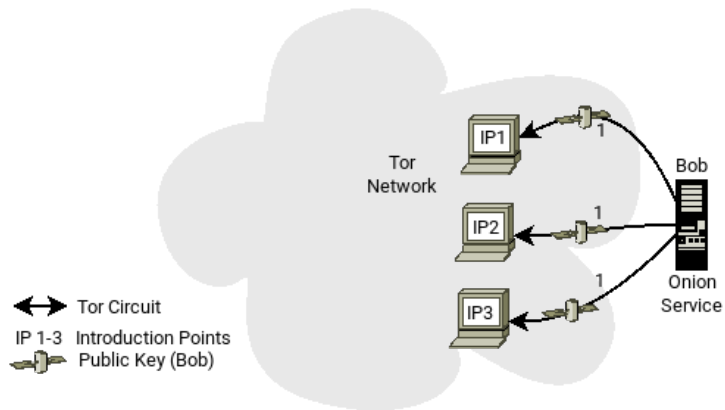
Netsurf licence: <https://www.netsurf-browser.org/about/licence.html>

XMPP trademark: <https://xmpp.org/about/xsf/jabber-trademark/usage-guidelines/>

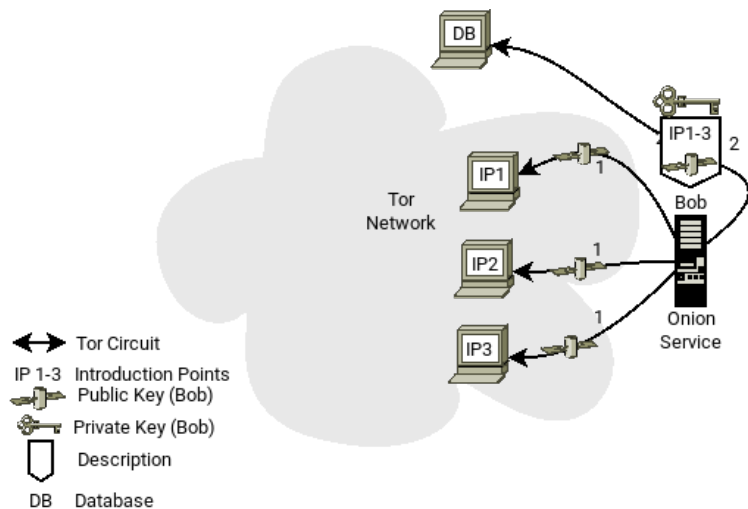
Λειτουργία

Βήματα λειτουργίας υπηρεσιών onion

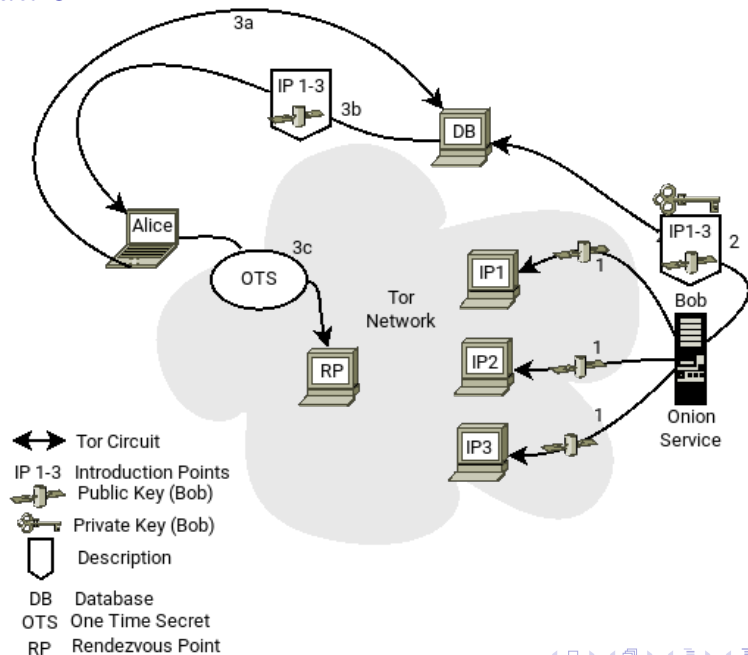
Βήμα 1



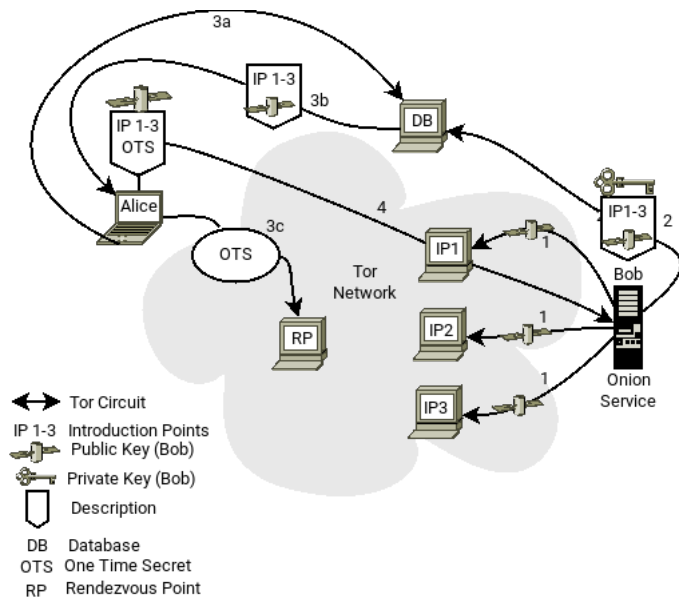
Βήμα 2



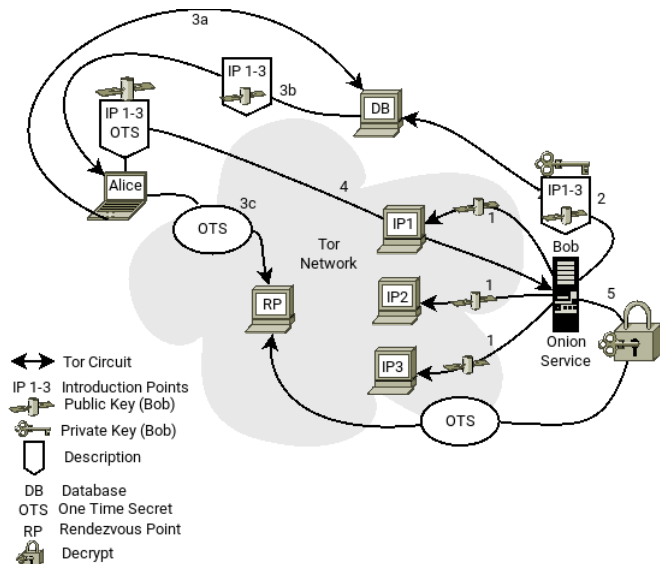
Βήμα 3



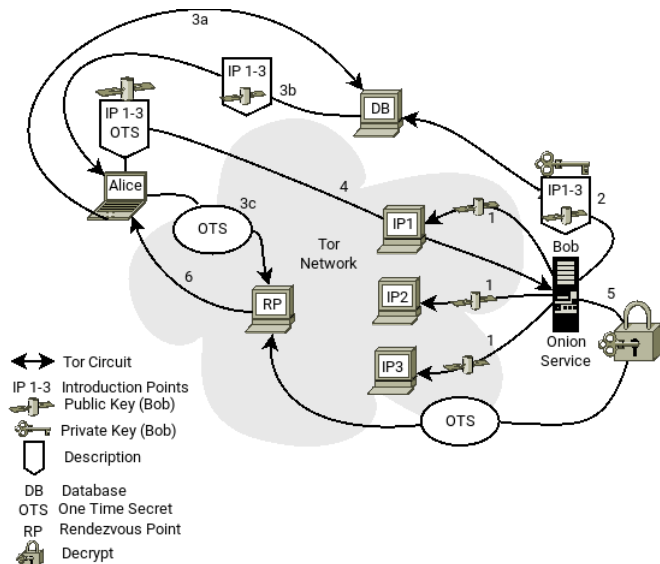
Βήμα 4



Βήμα 5



Βήμα 6



Το tor είναι ελεύθερο Λογισμικό² ³

Ο κώδικάς του είναι γνωστός ⇒ μπορεί να μελετηθεί και να εξακριβωθεί ότι λειτουργεί σύμφωνα με την τεκμηρίωση




²<https://www.gnu.org/philosophy/free-sw.html>

³https://support.torproject.org/about/#about_distribute-tor

Κενά ασφαλείας

Πέρα από τις DDoS επιθέσεις τα κενά ασφαλείας των υπηρεσιών ονιον υπάρχουν στις σελίδες:

- ▶ <https://gitlab.torproject.org/tpo/core/team/-/wikis/NetworkTeam/TROVE>
- ▶ <https://nvd.nist.gov/vuln/search>⁴

⁴Βάζοντας σαν όρο αναζήτησης το «onion services» 

Fin

Merci!!!