Εργαλεία κρυπτογράφησης κινησης δικτύου εν τάχυ

Σύγκριση εργαλειών και χρήση ανασκόπησης βιβλιογραφίας περιπτώσεων & μελέτης

Michail M

ΕΠΙΣΤΗΜΗΣ ΥΠΟΛΟΓΙΣΤΩΝ ΕΤΟΣ 3, ΑΣΦΑΛΕΙΑ ΥΠΟΛΟΓΙΣΤΩΝ ΚΑΙ ΔΙΚΤΥΩΝ



**SCHOOL OF ARCHITECTURE, COMPUTING & ENGINEERING**

*BSc in Computer Science*

**Michail Markou**

*CN6003 – COMPUTER AND NETWORK SECURITY*

**UEL NUMBER**

*2020732*

***Date***

11/11/2021

**Εργαλεία κρυπτογράφησης κίνησης δικτύου εν τάχυ**

Michail Markou

University of East London

Contents

[1. Περίληψη 1](#_Toc89657479)

[2. Εισαγωγή 1](#_Toc89657480)

[2.1. Κρυπτογραφημένη επικοινωνία δικτύου 1](#_Toc89657481)

[2.1.1. Πως δουλεύει 2](#_Toc89657482)

[2.1.2. VPN τύποι και περιπτώσεις χρήσης 5](#_Toc89657483)

[2.2. Ανώνυμη επικοινωνία δικτύου 11](#_Toc89657484)

[2.2.1. The Onion Routing – Πως λειτουργεί [47] 12](#_Toc89657485)

[2.2.2. Tor Hidden Services – Πως λειτουργεί 13](#_Toc89657486)

[2.2.3. Θέματα ευπάθειας & Ιατροδικαστική 15](#_Toc89657487)

[2.3. Το θέμα του νόμου προειδοποιήσεων 16](#_Toc89657488)

[3. Εργαλεία ασφαλείας 17](#_Toc89657489)

[3.1. OpenVPN 17](#_Toc89657490)

[3.1.1. Συντομία 17](#_Toc89657491)

[3.1.2. Υπέρ και κατά 17](#_Toc89657492)

[3.2. TOR 19](#_Toc89657493)

[3.2.1. Συντομία 19](#_Toc89657494)

[3.2.2. Υπερ και κατά 19](#_Toc89657495)

[3.3. Compare Results 20](#_Toc89657496)

[4. Ανασκόπηση βιβλιογραφίας ανάλυσης πραγματικής περίπτωσης 25](#_Toc89657497)

[4.1. Η μελέτη περίπτωσης 25](#_Toc89657498)

[4.1.1. Tor επιλογές 25](#_Toc89657499)

[4.1.2. torrc 25](#_Toc89657500)

[4.1.3. Λειτουργία κόμβου ρελέ 26](#_Toc89657501)

[4.1.4. κρυφή υπηρεσία 28](#_Toc89657502)

[References 30](#_Toc89657503)

[Appendix 36](#_Toc89657504)

[Glossary 36](#_Toc89657505)

[Figure 1 Internet connectivity options from end-user to tier 3/2 ISPs (tiers are ISP's) 4](#_Toc89630656)

[Figure 2 https://hackernoon.com/decentralized-vpn-the-evolution-of-tor-hkv3uix 5](#_Toc89630657)

[Figure 3 VPN Architecture Diagram with Routers/ VPN Concentrators 6](#_Toc89630658)

[Figure 4 VPN Architecture Diagram with UTM Appliances 7](#_Toc89630659)

[Figure 5 VPN Architecture Diagram using Wireless Controller 7](#_Toc89630660)

[Figure 6 https://www.bitvpn.net/blog/centralized-vs-decentralized-vpn/ 8](#_Toc89630661)

[Figure 7 virtual network device interfaces used by VPN clients to establish virtual instances of physical networking connections. 11](#_Toc89630662)

[Figure 8 https://tb-manual.torproject.org/about/ 15](#_Toc89630663)

[Figure 9 https://www.youtube.com/watch?v=QRYzre4bf7I 17](#_Toc89630664)

[Figure 10 Normal Onion Routing and Hidden Services 19](#_Toc89630665)

[Figure 11 World map of encryption laws and policies 20](#_Toc89630666)

[Figure 12 https://www.gp-digital.org/world-map-of-encryption/ 21](#_Toc89630667)

[Figure 13 https://restoreprivacy.com/vpn/openvpn-ipsec-wireguard-l2tp-ikev2-protocols/ 23](#_Toc89630668)

[Figure 14 Tor relay config in torrc 29](#_Toc89630669)

[Figure 15 Tor metrics 30](#_Toc89630670)

[Figure 16 torrc for hidden services 31](#_Toc89630671)

[Figure 17 Find your .onion address 32](#_Toc89630672)

# Περίληψη

Τα εργαλεία κρυπτογράφησης κίνησης για ανώνυμα δίκτυα επικοινωνιών γεννήθηκαν για να προστατεύσουν το απόρρητο, την ασφάλεια των επικοινωνιών μας στο διαδίκτυο, αποτρέποντας την παρακολούθηση, τη λογοκρισία και την ανάλυση κυκλοφορίας, είναι μακράν τα πιο διάσημα στην κατηγορία κρυπτογράφησης που χρησιμοποιούν όλοι για την προστασία της ιδιωτικής ζωής χωρίς διαφάνεια[[1]](#footnote-2).

Σε αυτά τα άρθρα, παρουσιάζουμε δύο βιομηχανικές βιομηχανικές λύσεις λογισμικού ανοιχτού κώδικα Δίκτυο ανωνυμοποίησης Tor & OpenVPN με μια συστηματική βιβλιογραφική ανασκόπηση σχετικά με την έρευνα που έγινε σε τύπους Tor και VPN που παρουσιάζουν την κατάσταση της τέχνης, την ιστορία, την αρχιτεκτονική, τα πρωτόκολλα και τη διαφορετική έρευνα προκλήσεις που πρέπει να αντιμετωπιστούν. Αυτή η περιεκτική ανασκόπηση αναπτύχθηκε από διάφορα άρθρα επιλογής και παρουσιάζει τα κύρια ευρήματα και περιπτώσεις χρήσης με τα πλεονεκτήματα και τα μειονεκτήματα κάθε εργαλείου, τους περιορισμούς και τα ζητήματα νόμου, δεν δημιουργήθηκαν όλα τα VPN εξίσου και περιλαμβάνουν πολλά στοιχεία, π.χ. πώς θα ωθήσουν την κυκλοφορία μέσα από τη σήραγγα και πολλά άλλα μοτίβα στρατηγικής. θα εξετάσουμε σε πλήρη προβολή τη γενική ιδέα, αλλά για να κατανοήσουμε ένα συγκεκριμένο εργαλείο πρώτα θα δούμε πώς λειτουργεί η υποκείμενη μηχανική του ενός VPN και το Tor βασίζεται σε μια αρχιτεκτονική VPN.

*Λέξεις-κλειδιά*: Εργαλεία ασφάλειας δικτύου; Tor; VPN; OpenVPN; Κρυπτογράφηση κυκλοφορίας; hidden services; επισκόπηση; αποκεντρωμένη δικτυακή υποδομή peer to peer;

# Εισαγωγή

## Κρυπτογραφημένη επικοινωνία δικτύου

Η τεχνολογία VPN ενισχύθηκε με μια πληθώρα τεχνικών υλοποίησης στην αγορά που ξεκίνησε με πολλά VPN, αλλά όλα είχαν την ίδια προσέγγιση ασφάλειας σε επίπεδο υλοποίησης αλλά όχι σε επίπεδο Επιχειρηματικής Πολιτικής εδώ διαφέρουν, αυτός είναι ο πραγματικός στόχος απορρήτου π.χ. κοινή χρήση αρχείων καταγραφής με τρίτους.

Ένα σύστημα VPN θα μπορούσε συνήθως να χρησιμοποιεί σήραγγες, τείχη προστασίας και διακομιστές μεσολάβησης και η αρχιτεκτονική του είναι είτε κεντρική είτε η νέα γενιά του VPN που βασίζεται στο WEB 3.0 αποκεντρωμένη.

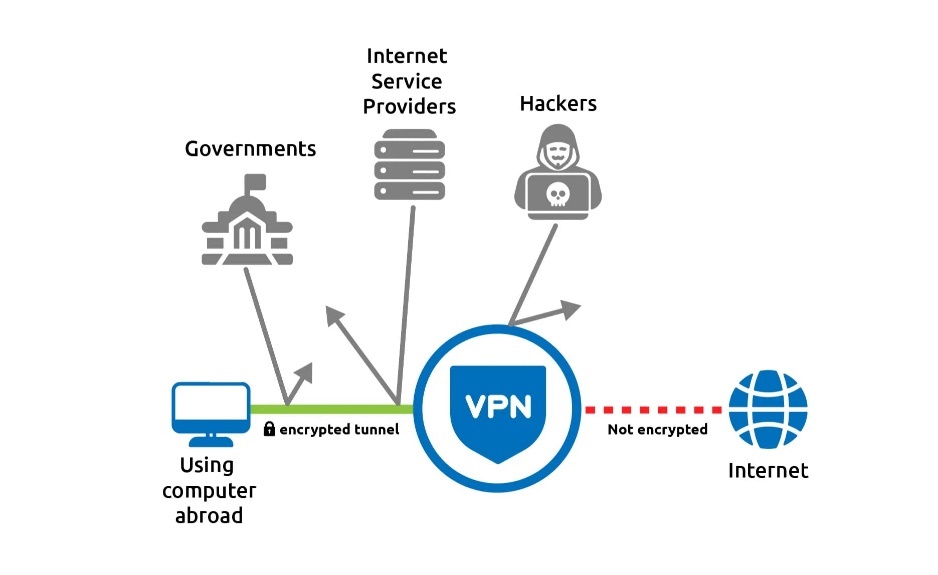


Figure 2 https://hackernoon.com/decentralized-vpn-the-evolution-of-tor-hkv3uix

### Πως δουλεύει

Οι οργανισμοί για να χρησιμοποιήσουν το Διαδίκτυο ως ιδιωτικό WAN, πρέπει να ξεπεράσουν δύο κύριες προκλήσεις. Πρώτον, τα δίκτυα επικοινωνούν συχνά με μια ποικιλία πρωτοκόλλων και όχι με IP, π.χ., IPX, επομένως υπάρχει αυτό το ζήτημα συμβατότητας χρησιμοποιώντας cross-platform, αλλά το Διαδίκτυο έχει σχεδιαστεί για να μεταφέρει και να επεξεργάζεται την κίνηση IP. Έτσι, τα VPN πρέπει να εφαρμόσουν έναν τρόπο για να περάσουν αυτήν την κίνηση πρωτοκόλλων που δεν είναι IP από το ένα δίκτυο στο άλλο. Το δεύτερο κύριο πράγμα είναι ότι τα πακέτα δεδομένων διασχίζουν το Διαδίκτυο ανοιχτά χωρίς καμία κρυπτογράφηση ή/και προστασία της ιδιωτικής ζωής "σε σαφές κείμενο" που μπορείτε να πείτε.

Κατά συνέπεια, όποιος μπορεί να δει την κίνηση στο Διαδίκτυο μπορεί επίσης να διαβάσει τα δεδομένα που περιέχονται στα πακέτα. Αυτό είναι το κύριο μέλημα της ιδιωτικής ζωής και της ασφάλειας, ειδικά από επιχειρηματική σκοπιά, όταν εμπιστευτικές επιχειρηματικές πληροφορίες διασχίζουν το Διαδίκτυο. Τα VPN μπορούν να εξαλείψουν αυτά τα εμπόδια χρησιμοποιώντας μια στρατηγική που ονομάζεται tunneling, η οποία αντί τα πακέτα να διασχίζουν το Διαδίκτυο ανοιχτά, τα πακέτα δεδομένων πρώτα κρυπτογραφούνται για ασφάλεια και στη συνέχεια ενσωματώνονται σε ένα πακέτο IP από το VPN και διοχετεύονται μέσω του Διαδικτύου.

«Για να επεξηγήσουμε την ιδέα, ας υποθέσουμε ότι εκτελούμε το NetWare σε ένα δίκτυο και ένας πελάτης σε αυτό το δίκτυο θέλει να συνδεθεί σε έναν απομακρυσμένο διακομιστή NetWare. Το κύριο πρωτόκολλο που χρησιμοποιείται με το παραδοσιακό NetWare είναι το IPX. Έτσι, για να χρησιμοποιήσετε ένα γενικό μοντέλο VPN επιπέδου-2, τα πακέτα IPX που συνδέονται για το απομακρυσμένο δίκτυο φτάνουν σε μια συσκευή εκκίνησης σήραγγας - ίσως μια συσκευή απομακρυσμένης πρόσβασης, έναν δρομολογητή ή ακόμα και έναν επιτραπέζιο υπολογιστή, στην περίπτωση απομακρυσμένου πελάτη-πελάτη συνδέσεις διακομιστή - που τις προετοιμάζει για μετάδοση μέσω Διαδικτύου. Ο εκκινητής σήραγγας VPN στο δίκτυο προέλευσης επικοινωνεί με έναν τερματιστή σήραγγας VPN στο δίκτυο προορισμού. Οι δύο συμφωνούν σε ένα σχήμα κρυπτογράφησης και ο εκκινητής της σήραγγας κρυπτογραφεί το πακέτο για ασφάλεια. Τέλος, ο εκκινητής VPN ενσωματώνει ολόκληρο το κρυπτογραφημένο πακέτο σε ένα πακέτο IP. Τώρα, ανεξάρτητα από τον τύπο του πρωτοκόλλου που αρχικά μεταδόθηκε, μπορεί να ταξιδέψει μόνο στο Διαδίκτυο IP. Και, επειδή το πακέτο είναι κρυπτογραφημένο, κανείς δεν μπορεί να διαβάσει τα αρχικά δεδομένα. Στο τέλος προορισμού, ο τερματιστής σήραγγας VPN λαμβάνει το πακέτο και αφαιρεί τις πληροφορίες IP. Στη συνέχεια αποκρυπτογραφεί το πακέτο σύμφωνα με το συμφωνημένο σχήμα κρυπτογράφησης και στέλνει το πακέτο που προκύπτει στον διακομιστή απομακρυσμένης πρόσβασης ή στον τοπικό δρομολογητή, ο οποίος περνά το κρυφό πακέτο IPX στο δίκτυο για παράδοση στον κατάλληλο προορισμό [28].”

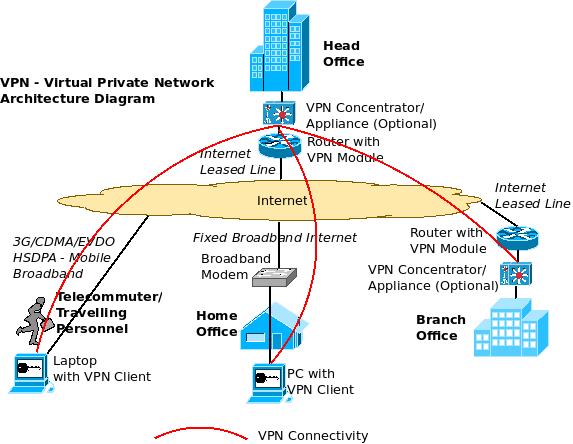


Figure 3 [VPN Architecture Diagram with Routers/ VPN Concentrators](https://excitingip.com/780/an-introduction-for-enterprise-vpn-virtual-private-network/)

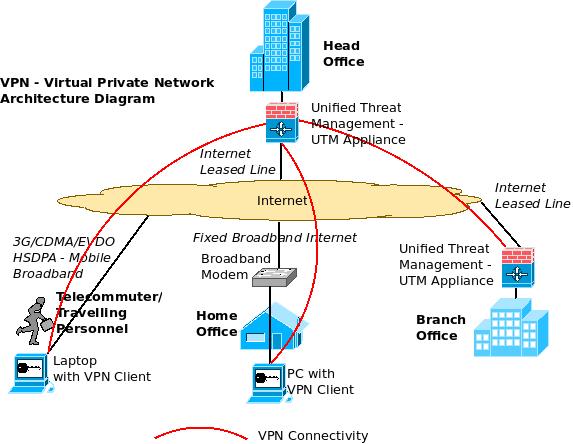


Figure 4 [VPN Architecture Diagram with UTM Appliances](https://excitingip.com/780/an-introduction-for-enterprise-vpn-virtual-private-network/)

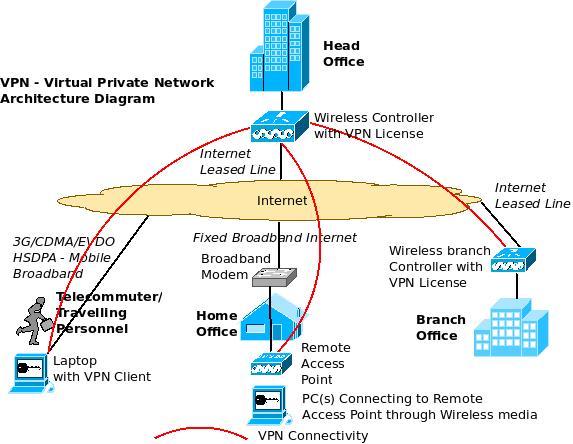


Figure 5 [VPN Architecture Diagram using Wireless Controller](https://excitingip.com/780/an-introduction-for-enterprise-vpn-virtual-private-network/)

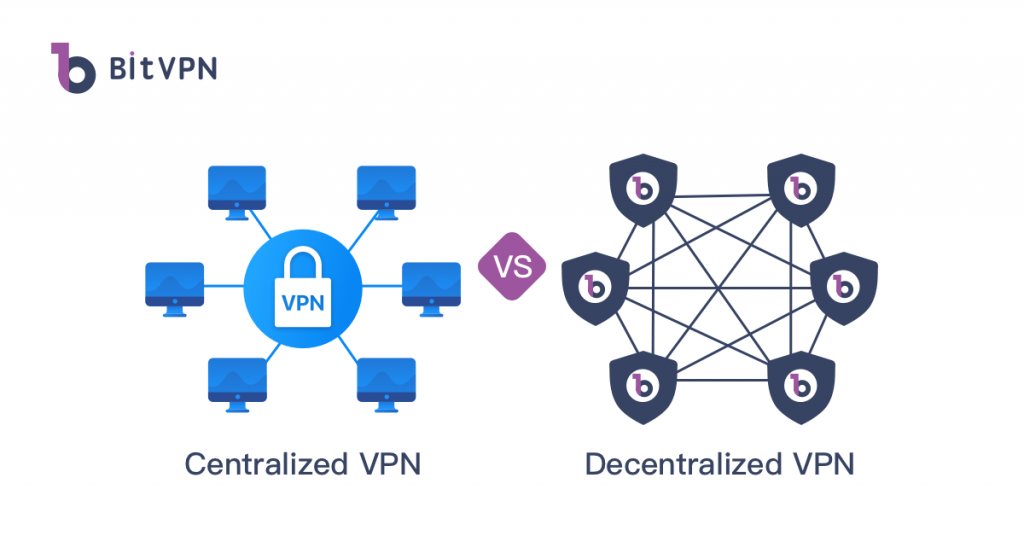


Figure 6 https://www.bitvpn.net/blog/centralized-vs-decentralized-vpn/

### VPN τύποι και περιπτώσεις χρήσης

#### Χαρακτηριστικά & Πλεονεκτήματα [29] [30] [31] [32] [33] [34]

• Κεντρικό VPN (Κλασικό)

• Αποκεντρωμένο VPN (υποστήριξη βάσει blockchain)

• Κρυπτογράφηση πριν από την πραγματική μετάδοση δεδομένων

• Βασισμένο σε πελάτες ή χωρίς πελάτες (με συγκεκριμένο λογισμικό ή απλώς πρόγραμμα περιήγησης)

• Κρυπτογράφηση δεδομένων εξερχόμενης διεπαφής (όχι μόνο η κίνηση των προγραμμάτων περιήγησης)[[2]](#footnote-3)

• Πληροφορίες ελέγχου/καταγραφής

• Αυτόματη γραμμή δημιουργίας αντιγράφων ασφαλείας Fail-Over

• Τα SSL VPN είναι καλύτερα για ανάκτηση καταστροφών/επιχειρησιακή συνέχεια, καθώς επιτρέπουν οπουδήποτε και ανά πάσα στιγμή πρόσβαση στα εταιρικά δίκτυα για εξουσιοδοτημένους χρήστες.

• Το VPN είναι επεκτάσιμο και η έννοια εξοικονόμησης κόστους μπορεί να επεκταθεί σε οποιοδήποτε υποκατάστημα/μεμονωμένο χρήστη που έχει πρόσβαση στο Διαδίκτυο μέσω Μισθωμένων Γραμμών Διαδικτύου/ Σταθερής Ευρυζωνικότητας/ Ευρυζωνικότητας κινητής τηλεφωνίας κ.λπ. Συνήθως προτιμάται έναντι της μισθωμένης γραμμής, καθώς οι μισθώσεις είναι ακριβές και η απόσταση μεταξύ των γραφείων αυξάνεται, το κόστος της μισθωμένης γραμμής αυξάνεται

• Εξοικονομεί χρόνο και έξοδα για υπαλλήλους που μετακινούνται από εικονικούς χώρους εργασίας

• Το VPN βοηθά στη συγκέντρωση όλων των πόρων πληροφορικής και επιτρέπει την κεντρική διαχείριση κρίσιμων πόρων πληροφορικής στα κεντρικά γραφεία του Data Center

• Παρέχετε εκτεταμένες συνδέσεις σε πολλές γεωγραφικές τοποθεσίες χωρίς τη χρήση μισθωμένης γραμμής.

• Βελτίωση του μηχανισμού ασφαλείας των δεδομένων με χρήση τεχνικών κρυπτογράφησης.

• Παρέχει ευελιξία στα απομακρυσμένα/ταξιδεύοντα γραφεία και τους υπαλλήλους να χρησιμοποιούν τους εταιρικούς πόρους της επιχείρησης στο intranet μέσω μιας υπάρχουσας σύνδεσης στο Διαδίκτυο σαν να είναι απευθείας συνδεδεμένοι στο δίκτυο με πρόσβαση λογισμικού πελάτη VPN (με τεχνολογίες SSL VPN, ακόμη και το λογισμικό πελάτη μπορεί να μην απαιτείται, απλώς ένα τυπικό πρόγραμμα περιήγησης).

• Τα VPN επιτρέπουν επιλεκτική πρόσβαση σε προμηθευτές και συνεργάτες μέσω μιας εξωτερικής πύλης, προκειμένου να αυξηθεί η αποτελεσματικότητά τους και να εκτελεστούν οι εργασίες πιο γρήγορα (extranet).

• Διακοπή ανεπιθύμητης συλλογής δεδομένων (π.χ. παρακολούθηση, διαφημίσεις).

• Ξεμπλοκάρισμα/παράκαμψη περιορισμών περιοχής για ψηφιακό περιεχόμενο (π.χ. λόγω πολιτικής χώρας)

• Ο πάροχος VPN θα μπορούσε να στείλει την επισκεψιμότητά σας μέσω Tor κατόπιν απαίτησής σας, ακόμη και χωρίς να χρησιμοποιήσετε κάποιο ειδικό πρόγραμμα περιήγησης Tor

• Πιθανή κρυπτογράφηση από άκρο σε άκρο (E2EE), π.χ. απλό κείμενο σε κρυπτογραφημένο κείμενο[[3]](#footnote-4)

#### Μειονεκτήματα

• Η σύνδεση VPN είναι αργή.

• Χωρίς ανωνυμοποίηση, εκτός εάν είναι dVPN

• Η σταθερότητα της σύνδεσης VPN ελέγχει κυρίως την επεκτασιμότητα του Διαδικτύου, παράγοντες εκτός του ελέγχου ενός οργανισμού.

• Η διαφορετική τεχνολογία VPN ενδέχεται να μην λειτουργεί μαζί λόγω ανώριμων προτύπων.

• Επειδή η σύνδεση διασχίζει δημόσιες γραμμές, είναι απαραίτητη η καλή κατανόηση των θεμάτων ασφάλειας του δικτύου και οι κατάλληλες προφυλάξεις πριν από την ανάπτυξη του VPN.

#### Τύποι

* VPN απομακρυσμένης πρόσβασης (για τελικούς χρήστες π.χ. κεντρικός υπολογιστής σε διακομιστή/δίκτυο/ιστότοπο)
  + Επίπεδο 2 VPN
  + Επίπεδο 3 VPN
  + Επίπεδο 4 VPN
* VPN από ιστότοπο σε ιστότοπο (για επιχειρήσεις, δρομολογητής σε δρομολογητή/δίκτυο σε δίκτυο)
  + Επίπεδο 2 VPN
  + Επίπεδο 3 VPN

#### Ευχρηστία & Ορολογία

• **Tunnel**: Η σήραγγα ή η ενθυλάκωση είναι μια τεχνική συσκευασίας ενός πακέτου δικτύου στο άλλο. Το ενθυλακωμένο πακέτο ονομάζεται πακέτο σήραγγας και το εξωτερικό πακέτο μεταφοράς. Μια εξωτερική κεφαλίδα IP προστίθεται στην αρχική κεφαλίδα και μεταξύ των δύο από αυτές τις κεφαλίδες βρίσκονται οι πληροφορίες ασφαλείας που αφορούν τη σήραγγα. Η εξωτερική κεφαλίδα περιλαμβάνει την πηγή και τους κόμβους προορισμού/τελικά σημεία της σήραγγας ενώ η εσωτερική κεφαλίδα προσδιορίζει τον αρχικό αποστολέα και τον παραλήπτη του πακέτου [35].

• **Client-to-site/Απομακρυσμένη πρόσβαση/χρήστης**: Το VPN επιτρέπει σε έναν χρήστη να συνδεθεί σε ένα ιδιωτικό δίκτυο και να έχει πρόσβαση στις υπηρεσίες και τους πόρους του εξ αποστάσεως. Η σύνδεση μεταξύ του χρήστη και του ιδιωτικού δικτύου γίνεται μέσω του Διαδικτύου και η σύνδεση είναι ασφαλής και ιδιωτική. Είναι χρήσιμο τόσο για επαγγελματίες όσο και για οικιακούς χρήστες.

Οι οικιακοί χρήστες ή οι ιδιώτες χρήστες VPN, χρησιμοποιούν κυρίως υπηρεσίες VPN για να παρακάμψουν τους περιφερειακούς περιορισμούς στο Διαδίκτυο και να αποκτήσουν πρόσβαση σε αποκλεισμένους ιστότοπους. Η συνείδηση ​​των χρηστών για την ασφάλεια του Διαδικτύου χρησιμοποιεί επίσης υπηρεσίες VPN για να βελτιώσει την ασφάλεια και το απόρρητό τους στο Διαδίκτυο.

Για παράδειγμα, ένας εταιρικός υπάλληλος, ενώ ταξιδεύει, χρησιμοποιεί ένα VPN για να συνδεθεί στο ιδιωτικό δίκτυο της εταιρείας του και να αποκτήσει απομακρυσμένη πρόσβαση σε αρχεία και πόρους στο ιδιωτικό δίκτυο [27].

• **Site-to-Site:** Το VPN ονομάζεται επίσης Router-to-Router VPN και χρησιμοποιείται κυρίως σε εταιρείες. Εταιρείες, με γραφεία σε διαφορετικές γεωγραφικές τοποθεσίες πάνω από μια σύνδεση Δικτύου Ευρείας Περιοχής (WAN) και χρησιμοποιούν VPN από ιστότοπο σε τοποθεσία για να συνδέσουν το δίκτυο μιας τοποθεσίας γραφείου με το δίκτυο σε άλλη τοποθεσία γραφείου. Όταν συνδέονται πολλά γραφεία της ίδιας εταιρείας χρησιμοποιώντας έναν τύπο VPN Site-to-Site, ονομάζεται VPN που βασίζεται σε Intranet. Όταν οι εταιρείες χρησιμοποιούν τον τύπο VPN από ιστότοπο σε τοποθεσία για να συνδεθούν στο γραφείο μιας άλλης εταιρείας, ονομάζεται VPN που βασίζεται σε Extranet. Βασικά, το VPN από ιστότοπο σε τοποθεσία δημιουργεί μια εικονική γέφυρα μεταξύ των δικτύων σε γεωγραφικά απομακρυσμένα γραφεία και τα συνδέει μέσω του Διαδικτύου και διατηρεί ασφαλή και ιδιωτική επικοινωνία μεταξύ των δικτύων.

Δεδομένου ότι το VPN από τοποθεσία σε τοποθεσία βασίζεται στην επικοινωνία δρομολογητή σε δρομολογητή, σε αυτόν τον τύπο VPN ένας δρομολογητής λειτουργεί ως πελάτης VPN και ένας άλλος δρομολογητής ως διακομιστής VPN. Η επικοινωνία μεταξύ των δύο δρομολογητών ξεκινά μόνο αφού επικυρωθεί ο έλεγχος ταυτότητας μεταξύ των δύο [27] [36].

• **VPN επιπέδου 4 (ανεξάρτητο από το δίκτυο)[[4]](#footnote-5):** Κατάλληλο για περιαγωγή με κινητές συσκευές (δεν αναφερόμαστε στην προοπτική του δικτύου κινητής τηλεφωνίας του ISP). Ένα VPN επιπέδου 4 είναι ανεξάρτητο από το δίκτυο καθώς βρίσκεται πάνω από το επίπεδο δικτύου 3. Η περίοδος λειτουργίας παραμένει ανοιχτή ανεξάρτητα από το εάν ο πελάτης αλλάζει μεταξύ δικτύων ή όχι, διατηρώντας μια συνεχή σύνδεση τόσο για τον χρήστη όσο και για την εφαρμογή. Δεδομένου ότι δεν υπάρχουν ειδικές απαιτήσεις για εξοπλισμό υποδομής δικτύου, ένα VPN επιπέδου 4 είναι επομένως πιο αξιόπιστο και ισχυρό [37].

• **VPN επιπέδου 3 (TUN):** Η γενική ιδέα είναι μια διεπαφή που ανήκει τουλάχιστον στο L3. Αυτό έχει χαμηλότερο κόστος επισκεψιμότητας καθώς το πακέτο μετάδοσης δεν θα περάσει τουλάχιστον από προεπιλογή (εξαρτάται από τον τρόπο με τον οποίο εφαρμόζεται η τεχνολογία του VPN επιπέδου 3 στον κώδικα) [38] [39]. (Εικόνα 7)

• **VPN επιπέδου 2 (TAP):** Η γενική ιδέα είναι μια διεπαφή που ανήκει τουλάχιστον σε συσκευή L2 έχει δυνατότητες L2 και κάνει γεφύρωση τμημάτων όπως διακόπτες. Αυτό μεταφέρει ολόκληρη τη μηχανική του επιπέδου 2 στη σήραγγα VPN, όπως εκπομπή, η εναέρια κίνηση να περάσει, αλλά μπορεί να έχει προβλήματα κλιμάκωσης και πάλι εξαρτάται από το πώς θα εφαρμοστεί στον κώδικα για να λειτουργήσει πόσες δυνατότητες ενός πραγματικού δικτύου επιπέδου 2 θα φέρει [38] [39] . (Εικόνα 7)

• **Κεντρικό VPN:** Κλασικό/Παραδοσιακό/Άμεσο VPN λειτουργεί σαν διακομιστής μεσολάβησης, υπάρχει ένας κύριος πάροχος που αποθηκεύει και καταγράφει τη διαδικτυακή σας δραστηριότητα (ή όχι). Το μειονέκτημα είναι ότι εξαρτάστε από την πολιτική κρίσης του Παρόχου για την κοινή χρήση των δεδομένων σας ή εάν δεχτεί επίθεση, η κεντρική προσέγγιση θα είναι μεγάλο πρόβλημα για το απόρρητό σας. Μια άλλη συναυλία αυτής της επιλογής είναι ο κλειστός πηγαίος κώδικας αυτής της φύσης ενός παρόχου VPN που πραγματικά δεν μπορείτε να καταλάβετε τι συμβαίνει στα παρασκήνια. Αυτή η ιδέα κεντρικού χαρακτήρα είναι αυτό που ονομάζεται αρχιτεκτονική WEB2 όπου μια κεντρική επιχειρηματική οντότητα μπορεί να έχει όλη την ισχύ των δεδομένων σας [33] [40] [41]. (Εικόνα 6)

• **Αποκεντρωμένο VPN (dVPN):** Η φύση αυτής της δομής δικτύου peer-to-peer εμποδίζει κάθε τύπο καταγραφής να είναι δυνατή. ο οποίος ήταν ο προηγούμενος ή ο επόμενος κόμβος ως μεταπήδηση πακέτων/διασταύρωση από τον έναν κόμβο στον άλλο. Είναι ένας κώδικας ανοιχτού κώδικα που σημαίνει διαφάνεια των ενεργειών του και υποστήριξη της εξελικτικής τεχνολογίας Blockchain που εφαρμόζεται στην αρχιτεκτονική WEB3 αλλά ταυτόχρονα κάθε κόμβος σε αντίθεση με το Tor που πληρώνει πληρώνετε ανά λεπτό κάθε κόμβο που διασχίζει η επισκεψιμότητά σας συνήθως με GAS Blockchain Ethereum. Ο καθένας παίζει ρόλο και μπορεί να είναι ο διακομιστής κατέχοντας κάτι, σε ένα περιβάλλον blockchain δεν ελέγχεστε από τη δράση μιας παγκόσμιας κύριας επιχειρηματικής οντότητας, επομένως υπάρχει διαφάνεια στο δίκτυο (επειδή μπορείτε να διαβάσετε τον κώδικα ανοιχτού κώδικα) αλλά όχι τις συναλλαγές του. Αυτό φέρνει την ανωνυμοποίηση σε οποιαδήποτε επίθεση σε επίπεδο μεσαίου κόμβου εκτός από τον πρώτο κόμβο μετάβασης ή τον τελευταίο κόμβο εξόδου. Όπως συμβαίνει με τις περισσότερες υποδομές P2P, όσο περισσότεροι συμμετέχοντες εντάσσονται στο δίκτυο, τόσο ισχυρότερο και πιο ισχυρό γίνεται.[33][40][41][42][43]**.** (Figure 6)

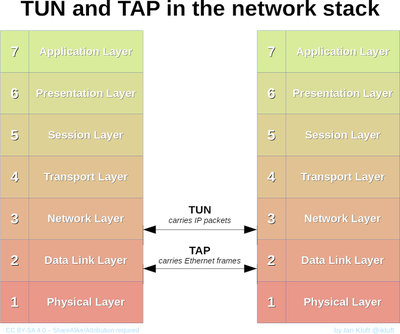


Figure 7 [virtual network device interfaces used by VPN clients to establish virtual instances of physical networking connections.](https://en.wikipedia.org/wiki/TUN/TAP)

#### Διάσημοι τύποι πρωτοκόλλων VPN [27] [29] [44] [45] [39] [32]

Οι παραπάνω δύο τύποι VPN βασίζονται σε διαφορετικά πρωτόκολλα ασφαλείας VPN που «κάθονται» πάνω από την ορολογία VPN. Καθένα από αυτά τα πρωτόκολλα VPN προσφέρει διαφορετικά χαρακτηριστικά και επίπεδα ασφάλειας και εξηγούνται παρακάτω:

• IPsec

o Επίπεδο 3 OSI

o Η πολιτική των τείχη προστασίας δικτύου είναι δυνατό να το αρνηθεί

o 2 τρόποι λειτουργίας: Λειτουργία μεταφοράς ή διάνοιξης σήραγγας

o Όχι πρωτόκολλο αλλά πλαίσιο/σειρά πρωτοκόλλων

o CIA και anti-replay

o Αλγόριθμοι κρυπτογράφησης (π.χ. 3DES, Diffie-helman)

o Σήραγγα VPN από ιστότοπο σε τοποθεσία

o Σήραγγα VPN από πελάτη σε τοποθεσία (απομακρυσμένος χρήστης).

o Πρόσβαση από ιστότοπο σε ιστότοπο (απαιτεί πελάτες που βασίζονται σε κεντρικούς υπολογιστές)

o Μεταξύ δύο διακομιστών για έλεγχο ταυτότητας και/ή κρυπτογράφηση της κυκλοφορίας

• L2TP

o Επέκταση PPTP

o Επίπεδο 2 σήραγγας Κυκλοφορία μέσω συνδέσεων στο επίπεδο τρία

o Απομακρυσμένο δίκτυο «Bridge» – ίδιο υποδίκτυο

o Δεν υπάρχει κρυπτογράφηση από προεπιλογή

o Μπορεί να χρησιμοποιήσει IPsec

• PPTP

o απαρχαιωμένο

• SSL VPN & TLS

o Κρυπτογράφηση για συγκεκριμένη εφαρμογή (π.χ. SMPT, FTP, XMPP, NNTP, HTTP/s)

o Επίπεδο εφαρμογής 7

o TLS νέα έκδοση του SSL

o Δεν χρειάζεται ειδικό πρόγραμμα-πελάτη λογισμικού για τις περισσότερες περιπτώσεις (βασισμένο σε πρόγραμμα περιήγησης/χωρίς πελάτη με προαιρετικό thin client) - απομακρυσμένη πρόσβαση

o Πύλη μέσω προγράμματος περιήγησης για πρόσβαση στην εφαρμογή

o Χρησιμοποιείται παντού επειδή η κυκλοφορία HTTPS είναι περισσότερο επιτρεπτή (δημόσια hotspot wi-fi)

• OpenVPN (περισσότερα για αυτό αργότερα)

o Ανοιχτού Κώδικα

o Από σημείο σε σημείο

o Από ιστότοπο σε τοποθεσία

o Προσαρμοσμένη ασφάλεια βάσει SSL/TLS

• SSH

o Οποιαδήποτε κρυπτογράφηση υπηρεσίας δικτύου

o Client-to-site/server

o Χρησιμοποιείται σε μηχανισμούς File Transfer Protocols

• VPLS

o Η γέφυρα L2 χρησιμοποιείται σε ISP ή σε μεγάλα εταιρικά δίκτυα. (Η παλιά μέθοδος ήταν L2TP. Μια περίπτωση χρήσης θα μπορούσε να είναι π.χ., από τελικό χρήστη ADSL σε διακομιστή απομακρυσμένης πρόσβασης ευρυζωνικής πρόσβασης (BRAS) [46]).

• MPLS L3 VPN

o Η επικοινωνία μεταξύ επιχειρηματικών υποκαταστημάτων με κρυπτογράφηση και προώθηση κίνησης μεταξύ τους από την πλευρά του ISP χρησιμοποιείται πάνω από οποιαδήποτε γραμμή από την προοπτική επιχείρησης/πελάτη που συνήθως μισθώνεται.

Κλπ.

|  |  |  |
| --- | --- | --- |
| **Χαρακτηρηστικά** | **SSL** | **IPSEC** |
| Έλεγχος ταυτότητας | Μονόδρομος έλεγχος ταυτότητας Αμοιβαίος έλεγχος ταυτότητας Ψηφιακό πιστοποιητικό | Αμοιβαίος έλεγχος ταυτότητας Ψηφιακό πιστοποιητικό |
| Κρυπτογράφηση | ισχυρός | Πολύ δυνατός |
| Τύπος κρυπτογράφησης | Μήκος κλειδιού 40 bit έως 128 bit | Μήκος κλειδιού 56 bit έως 256 bit |
| Πλήρης ασφάλεια | Ε2Ε | Άκρη δικτύου στον πελάτη, κρυπτογράφηση μόνο μεταξύ της πύλης VPN |
| Πρόσβαση | Εύκολη επιλογή ανά πάσα στιγμή, οπουδήποτε, Χωρίς πολιτική αποκλεισμού τείχους προστασίας | Περιορισμοί πρόσβασης στην καθορισμένη ελεγχόμενη πρόσβαση χρήστη. Η πολιτική τείχους προστασίας μπορεί να το αρνηθεί |
| Εγκατάσταση | Ανετα | Συγκρότημα |
| Εφαρμογή | Web, Κοινή χρήση αρχείων, Email | Όλα τα πρωτόκολλα βασίζονται σε υπηρεσία IP |
| Χρήστης | Πελάτες, συνεργάτες, προμηθευτές, χρήστες, απομακρυσμένοι χρήστες περισσότερα | Εσωτερικοί χρήστες |
| δίκτυο | Λειτουργεί στο στρώμα 4-7 | Λειτουργεί στο επίπεδο 3 |
| Τοποθεσία πύλης | Συνήθως αναπτύσσεται πίσω από το τείχος προστασίας | Συνήθως υλοποιείται στο τείχος προστασίας |
| Κλιμακούμενος/επεκτασιμος | Εύκολη διαμόρφωση και επέκταση | Εύκολη επέκταση στο τέλος του διακομιστή αλλά δύσκολη για τον πελάτη |
| Κόστος | Χαμηλός | Υψηλός |

## Ανώνυμη επικοινωνία δικτύου

Το Tor αποτελείται από ένα δίκτυο διακομιστών αναμετάδοσης που διευθύνονται από εθελοντές σε όλο τον κόσμο. Όταν οι άνθρωποι ακούν για το Onion Router (Tor) που είναι μια εφαρμογή της δρομολόγησης κρεμμυδιού (και ονομάζεται έτσι επειδή τα κρεμμύδια έχουν στρώματα και αυτό το πρωτόκολλο δικτύωσης έχει επίσης στρώματα) το πρώτο πράγμα που έρχεται στο μυαλό είναι το Dark-web aka Tor κρυφές υπηρεσίες, Deep-web, Services-web και είναι ένα διαφορετικό μέρος από το πώς λειτουργεί το Tor σε έναν εννοιολογικό όρο κρυπτογράφησης και προώθησης κίνησης. Το Tor διαφέρει από την εμπιστευτικότητα που συνήθως σχετίζεται με την κρυπτογράφηση (π.χ. κρυπτογράφηση μηνυμάτων) και ακόμα κι αν κάποιοι βλέπουν και λαμβάνουν αυτά τα μηνύματα δεν μπορούν να διαβάσουν τι είναι, αλλά μερικές φορές, δεν θέλουμε να τα βλέπουν οι άνθρωποι από την αρχή ότι στείλαμε μηνύματα. Παρακάτω συνοπτικά όλα εξηγούνται από προηγούμενες δηλώσεις. [47]

### The Onion Routing – Πως λειτουργεί [47]

Το Tor είναι μια ανώνυμη υπηρεσία επικοινωνίας χαμηλής καθυστέρησης που βασίζεται σε κύκλωμα [48] βασικά ένα δίκτυο επικάλυψης εικονικών σηράγγων σε ένα δημόσιο δίκτυο και όχι εγγενώς ένα δίκτυο peer-to-peer. Αυτό σας επιτρέπει να βελτιώσετε το απόρρητο και την ασφάλειά σας στο Διαδίκτυο (ανωνυμία) σε εφαρμογές που βασίζονται σε TCP, όπως η περιήγηση στο web, το ασφαλές κέλυφος και η ανταλλαγή άμεσων μηνυμάτων κ.λπ. Το Tor λειτουργεί (αναπηδώντας τις συνδέσεις σε διαφορετικούς δρομολογητές, ώστε να είναι δύσκολο να εντοπιστούν και να παρέχει ανωνυμία) στέλνοντας την επισκεψιμότητά σας μέσω τριών τυχαίων διακομιστών (επίσης γνωστών ως αναμετάδοσης) στο δίκτυο Tor μέσω του προγράμματος περιήγησης στη διεπαφή προσαρμογέων κεντρικού υπολογιστή που ενσωματώνεται από το Επίπεδο εφαρμογής σε πολλά επίπεδα κρυπτογράφησης, ανάλογη με την ενθυλάκωση στο μοντέλο του επιπέδου 7 OSI [49]. Το «κρεμμύδι» που προκύπτει είναι ένα πλήρως ενθυλακωμένο μήνυμα το οποίο στη συνέχεια δρομολογήθηκε από onion routers (διαμερισμένο σε μηνύματα κυψέλης εξίσου 512B στο onion network προκειμένου να δημιουργηθεί δυσδιάκριτη κίνηση κυκλοφορίας για να κάνει την παρακολούθηση σχεδόν αδύνατη τουλάχιστον μέσα στο δίκτυο Tor), μια σειρά από κόμβοι σε ένα δίκτυο με κάθε κόμβο να αφαιρεί ένα στρώμα από το «κρεμμύδι» και επομένως να αποκαλύπτει τον επόμενο προορισμό των δεδομένων. Το τελευταίο ρελέ στο κύκλωμα (το «ρελέ εξόδου») στέλνει στη συνέχεια την κυκλοφορία στο κοινό αφαιρώντας το τελευταίο επίπεδο ασφαλείας κρυπτογράφησης «onion» (έτσι μπορεί να λαμβάνετε ένα απλό κείμενο του αρχικού μηνύματος) στο Διαδίκτυο ενώ διατηρείτε ο αρχικός συντάκτης είναι ανώνυμος επειδή κάθε κόμβος στα δίκτυα γνωρίζει μόνο τους προηγούμενους και τους επόμενους κόμβους στη διαδρομή (εκτός από τον πρώτο κόμβο που γνωρίζει ποιος είναι στην πραγματικότητα ο αποστολέας, αλλά δεν γνωρίζει τον τελικό προορισμό) χωρίς πρόσθετη κρυπτογράφηση εκτός από εάν η αρχική υποδοχή δημιουργήθηκε σε μια κρυπτογραφημένη υπηρεσία (π.χ. HTTPS), οπότε ο τελευταίος κόμβος εξόδου είναι βασικά για λογαριασμό σας και ενεργεί ως διακομιστής μεσολάβησης.

Αυτό οδήγησε σε «επιθέσεις» στις οποίες η NSA εκτελεί διακομιστές προκειμένου να προσπαθήσει να είναι ο πρώτος και ο τελευταίος κόμβος στο δίκτυο. Εάν ο διακομιστής NSA είναι ο πρώτος κόμβος, γνωρίζει από πού προέρχεται το μήνυμα. Εάν ο διακομιστής NSA είναι ο τελευταίος κόμβος, γνωρίζει τον τελικό προορισμό και τι λέει το μήνυμα [50].

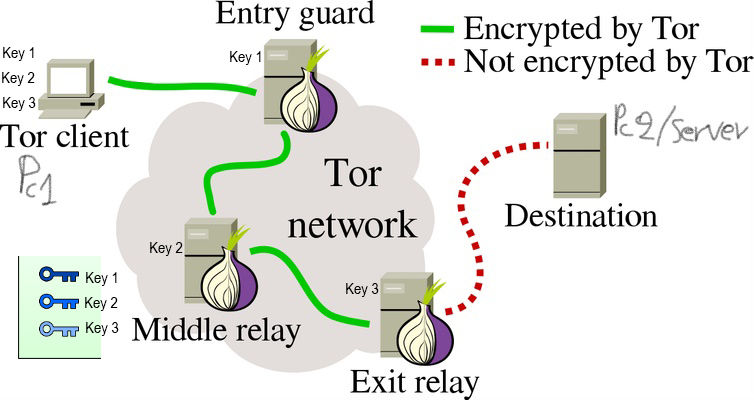


Figure 8 <https://tb-manual.torproject.org/about/>

Το Relay 1 (Είσοδος-φύλακας) γνωρίζει ποιος είστε, αλλά όχι πού πηγαίνετε.

Το Relay 2 (μεσαίος κόμβος) ξέρει μόνο πού να τον προωθήσει στο δίκτυο.

Το ρελέ 3 (κόμβος εξόδου) γνωρίζει πού πηγαίνετε, αλλά όχι ποιος είστε.

### Tor Hidden Services – Πως λειτουργεί

Το Tor Hidden Services (THS) (HS) γνωστό και ως Dark web προσπαθεί να κρύψει τη θέση IP ενός διακομιστή εντός του δικτύου Tor χωρίς κανέναν κόμβο εξόδου για να αποκαλύψει οποιαδήποτε λεπτομέρεια [51]. Μια κανονική χρήση του Tor με απλή ανωνυμοποίηση και μπορεί να απεικονιστεί στην εικόνα Σχήμα 8 και Εικόνα 10 ενώ το THS είναι Εικόνα 10.

Αυτές οι υπηρεσίες μπορούν να αναγνωριστούν επειδή οι διευθύνσεις τους έχουν τελειώσει σε ".onion" και οποιαδήποτε από αυτές απαιτεί από κάθε πολίτης να εκτελέσει τα πρωτόκολλα του ραντεβού για να επικοινωνήσει με την υπηρεσία με ανώνυμο τρόπο. Αυτός είναι ένας από τους λόγους που η THS συνδέεται με διάφορες παράνομες δραστηριότητες, αλλά «το Tor είναι κρίσιμη τεχνολογία όχι μόνο από την άποψη της προστασίας της ιδιωτικής ζωής, αλλά και για την υπεράσπιση του δικαιώματος δημοσίευσής μας» [52]. Ωστόσο, μπορεί να χρησιμοποιηθεί από δημοσιογράφους και για την παροχή ελευθερίας του λόγου προσφέρονται από οργανώσεις ανθρωπίνων δικαιωμάτων και καταγγελιών [53].

Για να επικοινωνήσει ένας χρήστης με ένα HS απαιτούνται κυρίως 3 κόμβοι που επιλέγονται από το HS και 3 από τον χρήστη, αλλά όσο μεγαλύτερο είναι το δίκτυο τόσο πιο ισχυρό μπορεί να είναι. Έτσι, σε αντίθεση με μια κανονική ανώνυμη επικοινωνία σε έναν ιστότοπο εκτός του δικτύου Tor (επιφάνεια | βαθύς ιστός) λαμβάνουν χώρα περισσότεροι κόμβοι. Ένα από αυτά τα 3 που επιλέγει ο χρήστης γίνεται το Rendezvous Point (RP) που με απλά λόγια αναμεταδίδει τα κρυπτογραφημένα μηνύματα του πελάτη στις υπηρεσίες και αντίστροφα.

«Με λίγη περισσότερη λεπτομέρεια, ένας χρήστης που θέλει να συνδεθεί ή να επισκεφτεί μια κρυφή υπηρεσία πρέπει να γνωρίζει τη διεύθυνση onion του, μια σειρά από 16 αλφαριθμητικούς χαρακτήρες. Στη συνέχεια, ο πελάτης αναζητά πληροφορίες σε έναν κόμβο καταλόγου (HSDir) που είναι βασικά ένας πίνακας κατακερματισμού (DHT) κατανεμημένος (μεταξύ όλων των κόμβων στο δίκτυο) που περιέχει τους περιγραφείς κάθε HS και βρίσκει ένα σημείο εισαγωγής (IP) που το κρυφό υπηρεσία έχει οριστεί προηγουμένως. Ταυτόχρονα, ο πελάτης επιλέγει επίσης έναν κόμβο που θα λειτουργεί ως RP και δημιουργεί ένα κύκλωμα σε αυτόν. Μόλις αυτός ο πελάτης συνδεθεί σε έναν από αυτούς τους κόμβους, η IP μεταδίδει μια ειδοποίηση στην κρυφή υπηρεσία, η οποία περιέχει τη διεύθυνση του σημείου του ραντεβού. Όταν η Hidden Service αναγνωρίσει το RP, δημιουργεί ένα νέο κύκλωμα σε αυτό και στέλνει ένα νέο μήνυμα στον πελάτη μέσω του IP, προκειμένου να κλείσει η αρχική σύνδεση με το IP και να διατηρήσουν και τα δύο το κύκλωμα χτισμένο προς το RP, η επικοινωνία επιτέλους εδραιώνεται. Τόσο οι IP όσο και το RP έχουν τρία ενδιάμεσα άλματα μεταξύ αυτών και του χρήστη και μεταξύ αυτών και του διακομιστή. Επομένως, κανείς δεν γνωρίζει την ταυτότητα κάθε μέρους. Επιπλέον, κάθε μήνυμα Tor είναι ένα σταθερό 512B που δημιουργεί ένα άλλο «στρώμα» δυσδιάκρισης της κίνησης ανάλυσης κυκλοφορίας του Tor μόνο μέσα στο δίκτυο. Τέλος, η επικοινωνία του HS και του χρήστη ταξιδεύει μέσω 6 hops και χρησιμοποιεί το RP ως ενδιάμεσο, έτσι ώστε να μην ταυτίζονται μεταξύ τους. Αυτό όσον αφορά την ανωνυμία πελάτη-διακομιστή τώρα ένας διακομιστής μπορεί να μην θέλει προστασία "απόκρυψης", αλλά θέλει μόνο προστασία του χρήστη, οπότε σε αυτήν την περίπτωση 3 IP θα εξαιρεθούν από τη διαδικασία ανταλλακτικών και θα μεταβούν απευθείας από ο διακομιστής σε RP.

Ως τελική σημείωση, οι κρυφές υπηρεσίες χρησιμοποιούν ένα άλλο διαφορετικό πρωτόκολλο WEB για τη διασύνδεση με υπηρεσίες πάνω από αυτές, που σημαίνει ότι είναι απλώς μια άλλη γλώσσα του ιστού ότι οι κανονικές υπηρεσίες WEB (Clearnet/surface/deep-web) όπως το google δεν έχουν εφαρμοστεί για να μιλήσετε σε αυτό το Dark πρωτόκολλο ιστού δεν υπάρχει API και δεν μπορεί να ευρετηριαστεί δεν μπορεί να μιλήσει στο Dark web. Εάν κάποιος που γνωρίζει πώς λειτουργεί το Dark web μπορεί εύκολα να δημιουργήσει ένα API που εξάγει τις κρυφές υπηρεσίες ευρετηριάζοντάς τες και δημοσιεύοντάς τες στο Clearnet (κανονικός ιστός) σε ένα δημόσιο φόρουμ (επίσης να σημειώσουμε ότι το Dark web μπορεί να ευρετηριαστεί επειδή είναι απλώς διαφορετικός ένας κανονικός ιστός από τα συνηθισμένα που γνωρίζουμε, π.χ. μηχανή αναζήτησης σκοτεινού ιστού ή Hidden wiki).

Για να συνοψίσουμε το HS απόκρυψη IP της φυσικής θέσης διακομιστή μέσω της χρήσης του πρωτοκόλλου onion, επιλέγοντας τυχαία ορισμένους ηλεκτρονόμους και χτίζοντας κυκλώματα σε αυτούς και ζητήστε τους να λειτουργήσουν ως IP λέγοντάς τους ένα δημόσιο κλειδί, στη συνέχεια η υπηρεσία onion συγκεντρώνει έναν περιγραφέα υπηρεσιών onion που περιέχει το κοινό του κλειδί (του διακομιστή) και μια περίληψη κάθε IP και υπογράφει αυτόν τον περιγραφέα με το ιδιωτικό του κλειδί. Στη συνέχεια, οι μεταφορτώσεις αυτού του περιγραφέα σε έναν κατανεμημένο πίνακα κατακερματισμού, όπως το torrent, παρακολουθούνται αυτές τις μέρες και αυτός ο περιγραφέας είναι η διεύθυνση onion, π.χ., dshjad786ndds.onion (αλφαριθμητικοί χαρακτήρες) εάν το όνομα V2 του είναι 16 ή 56 χαρακτήρων (για το V3) που είναι που προέρχονται από το δημόσιο κλειδί υπηρεσιών. Αυτές οι διευθύνσεις δεν χρησιμοποιούν DNS και δεν υπάρχει ούτε ένα για να τις καταργήσει ως κεντρική αρχή όπως αυτό που συμβαίνει στο Clearnet. Έτσι, για να επιλύσει αυτό το Tor χρησιμοποιεί μια συναίνεση/consensus των κόμβων των αρχών καταλόγου, οι οποίοι είναι ειδικοί αναμεταδότες στο δίκτυο Tor, διασκορπισμένοι και συγκεντρωμένοι, ενώ είναι υπεύθυνοι να ενημερώσουν και να διανείμουν μια κύρια λίστα όλων των αναμετάδοσης Tor κάνοντας ψηφοφορία και έτσι καταλήγοντας στη συναίνεση ( κοινή ψηφοφορία) αυτής της λίστας (μόνο οι διευθύνσεις v3 βρίσκονται σε αυτόν τον κατάλογο)[[5]](#footnote-6). Βασικά, είναι φύλακες πύλης που παρακολουθούν την κατάσταση των ηλεκτρονόμων Tor ως έγκυρων ή μη, σε απευθείας σύνδεση/εκτός σύνδεσης, κατάσταση εύρους ζώνης των ρελέ HS et al.

Περισσότερες λεπτομέρειες για το πρωτόκολλο Tor, τον διακομιστή καταλόγου, το πρωτόκολλο ραντεβού μπορείτε να βρείτε στις προδιαγραφές του Tor [54] και στο έγγραφο σχεδιασμού του [48]. [53]

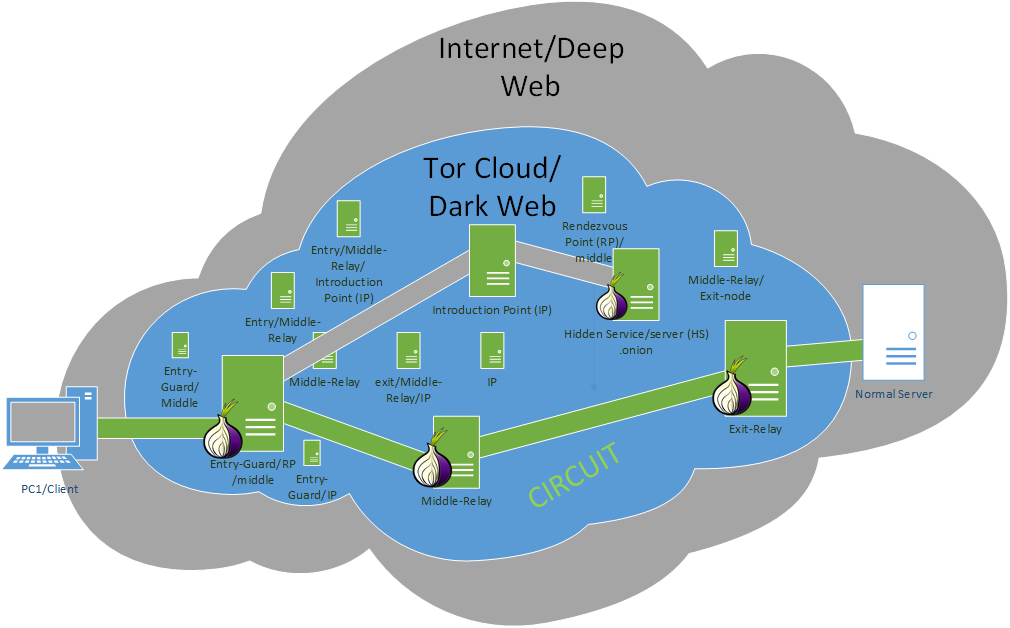


Figure 10 Normal Onion Routing and Hidden Services

### Θέματα ευπάθειας & Ιατροδικαστική

Η πραγματική ευπάθεια είναι ότι η επισκεψιμότητά σας είναι αδύναμη στον κόμβο Entry Guard και στον κόμβο Exit[[6]](#footnote-7) εάν κάποιος ακατάλληλος/παρακολουθεί αυτούς τους δύο κόμβους [[7]](#footnote-8) και συγχρονίζει προσεκτικά συμβάντα/μοτίβα που συνέβησαν σε διαφορετικά στάδια και στη συνέχεια αντιμετωπίζετε πρόβλημα (που σημαίνει ότι κατά την είσοδο και την έξοδο περισσότερες από 1 συνδέσεις/χρήστες θα μπορούσαν να είναι ζωντανοί και να εντοπίσουν το μοτίβο). Αλλά όπως συμβαίνει με όλα τα πράγματα, εάν κάποιος μπορεί να έχει τους πόρους για να τρέξει ένα μεγάλο μέρος του δικτύου τους δικούς του διακομιστές είτε για blockchain είτε Tor για κακοήθεις λόγους και να μετατρέψει την προσέγγιση Web3 σε Web2 με μια κεντρική οντότητα για να ελέγχει τα πάντα, τότε η ανωνυμία και η απώλεια απορρήτου Η προστασία είναι πάντα μια πιθανή απειλή [55].

## Το θέμα του νόμου προειδοποιήσεων

Κάθε φορέας επιβολής του νόμου σε μια χώρα έχει τους δικούς του κανόνες όσον αφορά τους περιορισμούς. Στην εποχή του WEB 2.0 όπου ο συγκεντρωτισμός είναι το κύριο πράγμα και η εξάρτηση, όπου τα πάντα ελέγχονται από μια ενιαία οντότητα, π.χ. κυβέρνηση, εταιρεία, τότε πρέπει να παίξετε με τους δικούς τους κανόνες. Σύμφωνα με τη Meta (πρώην Facebook), η E2EE καθυστερεί έως το 2023 λόγω των ενδιαφερομένων μερών για να διασφαλίσει ότι οι κακοί παράγοντες δεν κάνουν κατάχρηση του συστήματος [56].

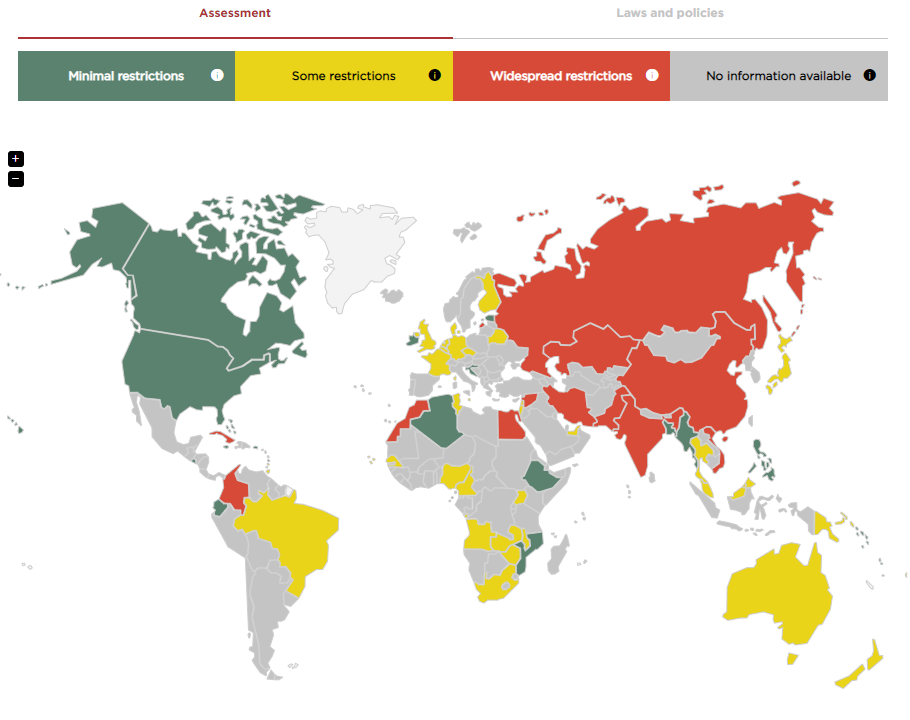


Figure 11 [World map of encryption laws and policies](https://www.gp-digital.org/world-map-of-encryption/)

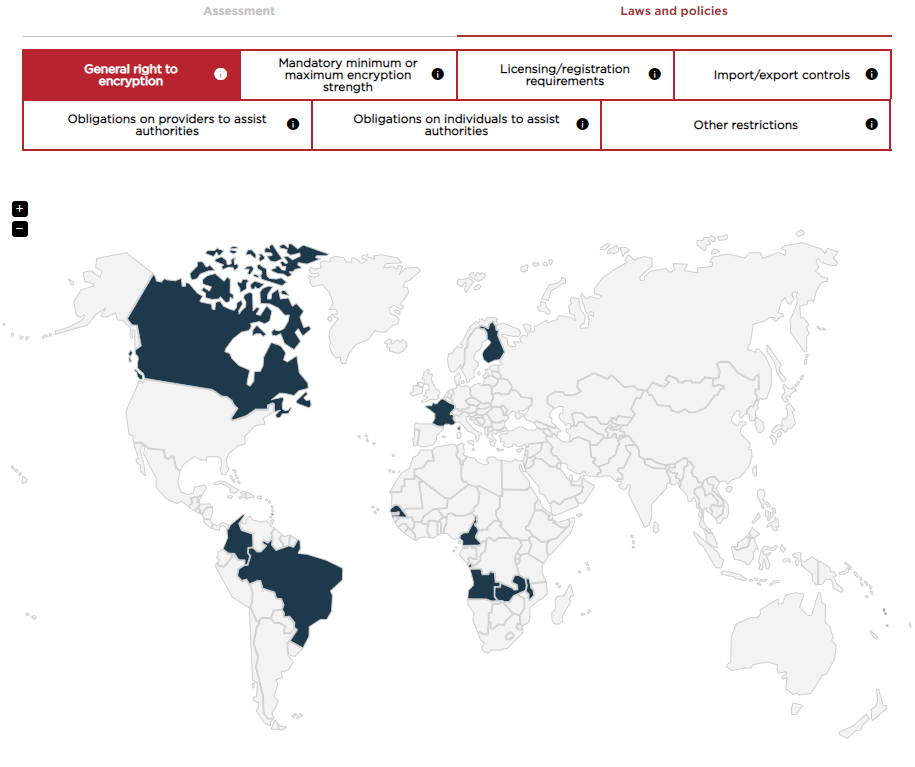


Figure 12 <https://www.gp-digital.org/world-map-of-encryption/>

# Εργαλεία ασφαλείας

## OpenVPN

### Συντομία

Ένα σύστημα VPN ανοιχτού κώδικα που σημαίνει διαφάνεια στο δίκτυο (μπορείτε να διαβάσετε τον κώδικά του) και υλοποιεί ασφαλή σύνδεση σημείου προς σημείο, τοποθεσίας σε τοποθεσία τόσο με εφαρμογές πελάτη όσο και με εφαρμογές διακομιστή[[8]](#footnote-9) ή οποιοδήποτε δίκτυο χρειάζεται το φυσικό ή οικοσύστημά σας στο cloud, είτε AWS, CGP, Azure κ.λπ. σε δρομολογημένες ή γεφυρωμένες διαμορφώσεις και εγκαταστάσεις απομακρυσμένης πρόσβασης. Κυκλοφόρησε για πρώτη φορά το 2001, γραμμένο σε C και είναι διαθέσιμο σε μια ποικιλία συστημάτων πλατφόρμας. Ορισμένος εξοπλισμός Δικτύωσης το υποστηρίζει από προεπιλογή ή μπορεί ακόμη και να εγκατασταθεί σε σύστημα υλικολογισμικού δρομολογητή Open/DD-Wrt Linux και είναι υπό άδεια GNU (GPLv2) [57].

### Υπέρ και κατά

#### Υπέρ [58] [59] [60]

• Ανοιχτού πηγαίου κώδικα

• Site-to-site

• Από πελάτη σε τοποθεσία

• Ε2ΕΕ[[9]](#footnote-10)

• Κρυπτογράφηση δεδομένων σε εξερχόμενη διεπαφή/προώθηση κατεύθυνσης ακόμη και χωρίς την κίνηση του προγράμματος περιήγησης

• Διεπαφές (L2/L3 - TAP/TUN)

• Ασφάλεια (κρυπτογράφηση υψηλής τεχνολογίας με κλειδιά κρυπτογράφησης υψηλών bit)

• Cross-platform

• Καλή συμβατότητα με τείχος προστασίας (οποιαδήποτε θύρα πλαισίων TCP/UDP, π.χ. με κάλυψη HTTPS)

• Φιλική μετάφραση διεύθυνσης δικτύου (NAT) (διέλευση)

• Perfect Forward Secrecy (αλλαγές μυστικών κλειδιών ανά πρόγραμμα-πελάτη/διακομιστή συνεδρίας)

• Χωρίς κόστος/τιμολόγηση για μη αυτόματη διαμόρφωση

#### Κατά [58]

• Συγκεντρωτική.

• Απαιτεί πρόσθετο πρόγραμμα-πελάτη λογισμικού

• Πολύπλοκη χειροκίνητη διαμόρφωση

• Δεν υπάρχει ελεύθερη περιαγωγή για φορητές συσκευές σε περίπτωση που αλλάξει το IP L3 η σύνδεση/περίοδος σύνδεσης θα χαθεί, καθώς από την άποψη της κινητής τηλεφωνίας δεν υπάρχει πρόβλημα επειδή δεν υπάρχει αλλαγή διεύθυνσης L3 μεταξύ αλλαγής δικτύου ραδιοπρόσβασης (RAN).

• Κόστος για έτοιμη λύση GUI (άδεια)

• Περιορισμός στον αριθμό των διακομιστών και των συνδέσεων (δωρεάν έκδοση)

• Εύρος ζώνης ή/και καθυστέρηση λόγω πολλών γενικών εξόδων και κρυπτογραφήσεων (ο χώρος χρήστη είναι πιο εμφανής για να προκαλέσει προβλήματα εδώ, όχι πάντα ως μειονεκτήματα)[[10]](#footnote-11)

• Υποστήριξη διακομιστή μεσολάβησης (αν δεν βρεθεί συμβατός διακομιστής μεσολάβησης)

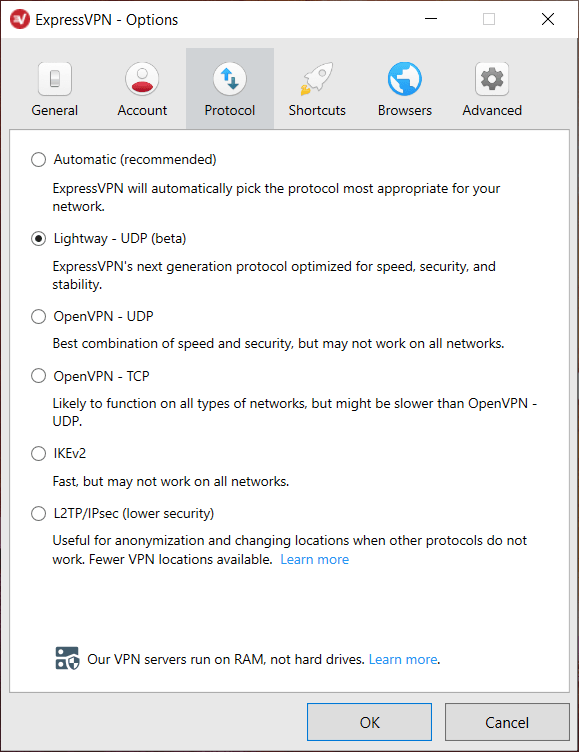


Figure 13 https://restoreprivacy.com/vpn/openvpn-ipsec-wireguard-l2tp-ikev2-protocols/

## TOR

### Συντομία

Το Tor, συντομογραφία του The Onion Router, είναι δωρεάν λογισμικό ανοιχτού κώδικα για την ενεργοποίηση της ανώνυμης επικοινωνίας. Κατευθύνει την κυκλοφορία του Διαδικτύου μέσω ενός δωρεάν, παγκόσμιου, εθελοντικού δικτύου επικάλυψης, για απόκρυψη της τοποθεσίας και της χρήσης ενός χρήστη από οποιονδήποτε πραγματοποιεί παρακολούθηση δικτύου ή ανάλυση κυκλοφορίας. Η χρήση του Tor καθιστά πιο δύσκολο τον εντοπισμό της δραστηριότητας του Διαδικτύου στον χρήστη. Η επιδιωκόμενη χρήση του Tor είναι να προστατεύει το προσωπικό απόρρητο των χρηστών του, καθώς και την ελευθερία και την ικανότητά τους να διεξάγουν εμπιστευτική επικοινωνία, διατηρώντας τις δραστηριότητές τους στο Διαδίκτυο χωρίς παρακολούθηση [14]. Είναι γραμμένο σε C, Python, Rust και είναι διαθέσιμο για πολλές πλατφόρμες.

### Υπερ και κατά

#### Υπέρ [34] [61] [62]

• Ανοιχτή πηγή

• Ανωνυμοποίηση

• χωρίς κόστος

• Αποκεντρωμένη χωρίς blockchain για πληρωμές

• Χωρίς έλεγχο

• Ασφαλής περιήγηση (HTTPS παντού, NoScript και κρυπτογραφημένα δεδομένα)

• Δημοκρατικές δραστηριότητες (μπορείτε να δημοσιεύσετε οτιδήποτε κρύβεστε)

• Deep web access (Deep web και αποκλεισμένοι ιστότοποι από κανονικές μηχανές αναζήτησης)

• Ιστότοποι .onion (προσβάσιμοι μόνο μέσω του προγράμματος περιήγησης του Tor και σχετίζονται με το deep/dark web)

• Τα επίπεδα κρυπτογράφησης που προστέθηκαν δεν επιβραδύνουν το Tor. Στη χρονική σήμανση [47] βίντεο 12:50 – 14:00

#### Κατά

• Αργή σύνδεση σε σύγκριση με τα κανονικά προγράμματα περιήγησης

• Οι κόμβοι εξόδου δεν κρυπτογραφούν την κυκλοφορία

• Παράνομη χρήση

• Ο χρόνος εκκίνησης του προγράμματος περιήγησης είναι πιο αργός ενώ αναζητά τους διαθέσιμους διακομιστές κόμβου φρουράς για σύνδεση.

• Ορισμένα σενάρια είναι μπλοκαρισμένα, απενεργοποιήστε ορισμένες διαδικτυακές λειτουργίες

• Κρυπτογράφηση δεδομένων μόνο μέσω της κίνησης του προγράμματος περιήγησης και εντός του δικτύου Tor[[11]](#footnote-12)

• Όχι E2EE[[12]](#footnote-13)

## Compare Results

**OpenVPN vs Tor**

|  |  |  |  |
| --- | --- | --- | --- |
| **Κριτήρια** | **dVPN (πιθανον στο μελλον?)** | **OpenVPN** | **Tor** |
| *Ανοιχτή πηγή* | **+** | **+** | **+** |
| *Γρήγορη ταχύτητα* | **+, -** | **+ , -** | **-** |
| *Εύκολο στη ρύθμιση* | **+ , -** | **-** | **+** |
| *Εύκολο στην εκμάθηση* | **+ , -** | **-** | **+** |
| *Διεπαφές δικτύου* | **+** | **+** | **-** |
| *Επεκτασιμότητα* | **+** | **+** | **+ , -** |
| *Ανωνυμοποίηση* | **+** | **-** | **+** |
| *Κρυπτογραφημένες συνδέσεις* | **+** | **+** | **+** |
| *Ενθυλάκωση πακέτων Κρυπτογράφηση* | **+** | **+** | **+** |
| *Κρυπτογράφηση ωφέλιμου φορτίου δεδομένων* | **+ (any service is behaving like “using” “HTTPS” due to blockchain nature)** [63][64] | **yes, if the target service is on site** | **-** |
| *Προστατεύει όλες τις διαδικτυακές συνδέσεις* | **+, - (e.g., site-to-site or host-to-host)** | **+ , -** | **-** |
| *Εξασφαλίζει την ιδιωτικότητα* | **+** | **+ , -** | **+** |
| *Κρυπτογράφηση από άκρο σε άκρο (E2EE)* | **+** | **Only for site-to-site and target service to be inside on target site** | **-** |
| *Αποκεντρωμένοι κόμβοι peer-to-peer* | **+** | **-** | **+** |
| *Ευελιξία στο Οικοσύστημα Επιχειρηματικών Δικτύων* | **+** | **+** | **-** |
| *Υποστήριξη επιχειρήσεων (εάν μπορεί να εφαρμοστεί)* | **+** | **+** | **+ , -** |
| *Υποστήριξη τελικού χρήστη* | **+** | **+** | **+** |
| *Δύσκολο να εντοπιστεί* | **+** | **+ , -** | **+** |
| *Φιλικό προς το χρήστη* | **+ , -** | **+ , -** | **+** |
| *Ξεκλειδώστε περιεχόμενο ροής* | **+** | **+** | **Yes, but not usable due to its speed** |
| *Βαθύς ιστός* | **+** | **+** | **+** |
| *Dark web (κρυφές υπηρεσίες)* | **+, -** | **-** | **++** |
| *Περιαγωγή (όχι από την πλευρά του ISP RAN κινητής τηλεφωνίας)* | **? (Depends on implementation)** | **-** | **-** |
| *Εύκολη επιλογή κόμβου εξόδου* | **+** | **+** | **-** |
| *Πρότυπο της βιομηχανίας* | **+** | **+** | **+** |
| *Χωρίς κεντρικό έλεγχο/καταγραφή* | **+** | **-** | **+** |
| *Υποστήριξη προϊόντος και κοινότητας* | **+ , -** | **+** | **+** |
| Κόστος/Τιμολόγηση | **Pay as you go** | **Free or subscription** | **Free** |

#### **Σημειώσεις προς λήψη & Επεξήγηση επιλεγμένων κριτηρίων**

Όταν συγκρίνουμε προϊόντα, πρέπει να έχουμε κατά νου ορισμένα βασικά πράγματα.

Εάν είναι αρκετά μεγάλο εκεί έξω, ώστε να μπορούμε να βασιστούμε σε αυτήν ως επιχείρηση και να το προσαρμόσουμε υπό τον γενικό όρο «βιομηχανικό πρότυπο» από τα χαρακτηριστικά του, την υιοθέτηση και προσαρμογή επιχειρηματικής στρατηγικής, την υποστήριξη προϊόντων και τη διαθεσιμότητα προϊόντων σε πολλές μορφές.

• **Ανοιχτού κώδικα:** Για μάθηση και ανάπτυξη και κατανόηση. Μοιραστείτε == φροντίδα

• **Γρήγορη Ταχύτητα:** Σύνδεση με μέτρηση της ταχύτητας του Διαδικτύου με βάση την καθυστέρηση ανάλογα με τον αλγόριθμο κρυπτογράφησης.

• **Εύκολη ρύθμιση:** Δυνατότητα χρήσης εκτός συσκευασίας ή πόσο περίπλοκη μπορεί να είναι με τη μη αυτόματη διαμόρφωση.

• **Εύκολη εκμάθηση:** Αφαίρεση του πολύπλοκου υποκείμενου συστήματος + το προσεγγίζουν περισσότεροι πελάτες.

• **Διεπαφές δικτύου:** Εύκολη διαμόρφωση και προσθήκη οποιασδήποτε συσκευής επικοινωνίας δικτύου εικονικού ή φυσικού προγράμματος οδήγησης πυρήνα.

• **Επεκτασιμότητα:** Μπορεί εύκολα να επεκταθεί κατά απαίτηση ή/και προσβασιμότητα μεταξύ πλατφορμών.

• **Ανωνυμοποίηση:** Απόκρυψη εντελώς δραστηριότητας ατόμων

• **Κρυπτογραφημένες συνδέσεις:** Ρύθμιση καναλιού και κρυπτογράφησης ροής δεδομένων

• **Κρυπτογράφηση ενθυλάκωσης πακέτων:** Κρυπτογράφηση στο Επίπεδο 3

• **Κρυπτογράφηση ωφέλιμου φορτίου δεδομένων:** Κρυπτογράφηση επιπέδου ωφέλιμου φορτίου 5-7

• **Προστατεύει όλες τις διαδικτυακές συνδέσεις**: Αυτόματη κρυπτογράφηση όλης της εισερχόμενης κίνησης για εξερχόμενους προορισμούς με κρυπτογραφημένη σήραγγα.

• **Εξασφαλίζει το απόρρητο:** Κρυπτογράφηση του περιεχομένου της δραστηριότητας.

• **Κρυπτογράφηση από άκρο σε άκρο (E2EE):** Σχήμα κρυπτογράφησης προορισμού εφαρμογής από την πηγή στο στόχο υπηρεσίας (όπως απλό SSL ή SSL μέσω σύνθετης αλυσίδας μπλοκ).

• **Αποκεντρωμένοι κόμβοι peer-to-peer:** Δεν ελέγχονται από μία μόνο οντότητα.

• **Ευελιξία στο Οικοσύστημα Επιχειρηματικού Δικτύου:** Υποστήριξη επιχειρήσεων + επεκτασιμότητα σε υποδομή ή λύση λογισμικού ως υπηρεσίας (SaaS).

• **Υποστήριξη επιχειρήσεων (εάν μπορεί να εφαρμοστεί):** Αρχιτεκτονική εταιρικών λύσεων προσαρμογής σε επίπεδο δικτύου.

• **Δύσκολος εντοπισμός:** Εφαρμογή των πραγματικών προδιαγραφών στην αρχιτεκτονική για την απόκρυψη πληροφοριών.

• **Φιλικό προς το χρήστη:** Διαισθητικός και συναρπαστικός σχεδιασμός (G)UI για προσβασιμότητα αλληλεπίδρασης ανθρώπου-υπολογιστή (HCI).

• **Ξεκλείδωμα περιεχομένου ροής:** Παράκαμψη τοπικών γεωγραφικών περιορισμών

• **Deep web:** Δυνατότητα πλήρους πρόσβασης στον επιφανειακό ιστό

• **Dark web (κρυφές υπηρεσίες):** Ένα web αντίγραφο ελευθερίας και ανωνυμίας

• **Περιαγωγή (όχι από την πλευρά του ISP RAN κινητής τηλεφωνίας):**

• **Εύκολη επιλογή κόμβου εξόδου:** Ευκολότερη πρόσβαση σε απομακρυσμένες γεωγραφικές τοπικές φυσικές υπηρεσίες.

• **Industry Standard:** Απλώς λειτουργεί για τα πάντα, επομένως η προσαρμογή για όλους είναι ευπρόσδεκτη. Το οικοσύστημα επεκτείνεται.

• **Χωρίς κεντρικό έλεγχο/καταγραφή:** Δεν υπάρχει ιστορικό και αποθηκευμένα δεδομένα οποιασδήποτε συναλλαγής ή αλληλεπίδρασης.

• **Υποστήριξη προϊόντος και κοινότητας**: Βελτίωση και βελτίωση (λογισμικό) και υποστήριξη πελατών με λύσεις και πρόσθετα/εργαλεία για ένα ισχυρό οικοσύστημα.

• **Κόστος/Τιμολόγηση:** Εύκολη πρόσβαση για εκπαιδευτική ή εταιρική χρήση

#### **Αποτελέσματα**

Το δώρο που πρέπει να πάρετε είναι ότι δεν υπάρχει τέλεια λύση όλα μπορούν να ικανοποιήσουν κάποιον και να δυσαρεστήσουν κάποιον άλλο. Κάθε εργαλείο έχει τις χρήσεις του στο σωστό σημείο και κάτω από ένα προβλεπόμενο δίκτυο σχεδιασμένο στρατηγικά. Αφορά το τι θέλει ένας πελάτης ή/και ενδιαφερόμενος σε ένα έργο. Θα μπορούσαν να λειτουργήσουν ως συμπληρωματική λύση μεταξύ τους για να ενισχύσουν ακόμη περισσότερο την ασφάλεια.

Το OpenVPN είναι κατάλληλο για έναν απλό χρήστη που θέλει απόρρητο χωρίς ανωνυμία και οποιοδήποτε κόστος ή για μια επιχείρηση που εφαρμόζει πρόσβαση VPN intranet/extranet (απομακρυσμένη πρόσβαση) στους υπαλλήλους του ή για ολόκληρη σύνδεση από ιστότοπο σε τοποθεσία γεφύρωση και δρομολόγηση για τη συγχώνευση του χάσματος της ασύνδετης μορφής ή δίκτυο πολιτικής και κάνοντάς το σαν τμήμα του επιπέδου 2, μοιράζοντας το τμήμα ή το επίπεδο 3, δηλαδή, εκτελώντας δρομολογητές γειτονίας με γειτονιές μέσω της σήραγγας. Το κύριο πραγματικό μειονέκτημα είναι ότι δεν χρησιμοποιεί E2EE, επομένως ο χρήστης πρέπει να γνωρίζει το επίπεδο υπηρεσίας-στόχου και ο απομακρυσμένος διακομιστής VPN είναι Κεντρικός και θα μπορούσε ενδεχομένως να σας καταγράψει (αποθηκεύοντας τα δεδομένα σας) για κοινή χρήση τρίτων, π.χ. εξόρυξη δεδομένων, κυβερνητικός κατάσκοπος, χάκερ (μια επίθεση).

Το Tor από την άλλη πλευρά είναι πολύ ισχυρό για την ανωνυμία κάτι που το OpenVPN δεν παρέχει νόημα για έναν χρήστη που θέλει να είναι αόρατος τουλάχιστον από κατασκόπους στη μέση[[13]](#footnote-14). Ωστόσο, είναι αρκετά ακατάλληλο για εταιρικά δίκτυα που θέλουν απόρρητο, είναι περισσότερο από τον χρήστη και όχι από την επιχείρηση, αλλά θα μπορούσε να γίνει.

Ένας συνδυασμός και των δύο λύσεων (Tor + OpenVPN) διατίθεται σε δύο γεύσεις (προσεγγίσεις) [43]:

* + - VPN on Tor (source host (bind to VPN) -> Tor -> ISP -> VPN (exit) -> Target service)
      * Συνδέστε το Tor και στη συνέχεια χρησιμοποιήστε ένα VPN: Απαιτεί πολύπλοκη μη αυτόματη διαμόρφωση. Ο διακομιστής VPN σας λειτουργεί ως ο τελικός κόμβος εξόδου και ο κόμβος εξόδου Tors θα μεταφέρει το πακέτο ακόμα κρυπτογραφημένο χωρίς να διακυβεύεται η δραστηριότητά σας (λόγω VPN).
      * ISP μπορεί να σας δει ότι χρησιμοποιείτε το Tor, αλλά δεν θα μπορεί να σας εντοπίσει ενώ κρατάτε τη διεύθυνση IP σας κρυμμένη από την υπηρεσία VPN για περαιτέρω έλεγχο/καταγραφή.
      * Εάν υπάρξει επίθεση στον κόμβο εξόδου του Tor, το πακέτο σας θα παραμείνει κρυπτογραφημένο επειδή ο κόμβος δεν θα μπορεί να πει τη δραστηριότητά σας λόγω VPN.
    - Tor over VPN (source host -> VPN -> ISP -> Tor (exit) -> Target service)
      * Συνδεθείτε στο VPN σας και στη συνέχεια χρησιμοποιήστε το Tor: Με αυτόν τον τρόπο κρυπτογραφείτε την κίνηση προτού εισέλθει στο δίκτυο Tor και επίσης αποκρύπτετε τη διεύθυνση IP σας στον κόμβο εξόδου του Tor
      * ISP δεν μπορεί να πει ότι χρησιμοποιείτε Tor
      * Ο πάροχος VPN θα παρακολουθεί τη δραστηριότητα του Tor και θα μπορεί να καταγράφει. Μια λύση είναι η χρήση ενός αποκεντρωμένου VPN, το οποίο δεν μπορεί να διατηρήσει αρχεία καταγραφής χρηστών.

Ενώ το κανονικό VPN προσφέρει προστασία στους χρήστες του (με αντίτιμο), ο πραγματικός αγώνας κατά της παρακολούθησης και της λογοκρισίας είναι κοινός, επειδή οι σημερινοί πάροχοι δεν κάνουν τίποτα για να αντιμετωπίσουν τα ελαττώματα υποδομής του Διαδικτύου, επομένως δεν υπάρχει ασυλία στον εταιρικό ή κυβερνητικό έλεγχο. [43]

Δεν υπάρχει μια ενιαία λύση για όλα τα μεγέθη ή ένας αληθινός μηχανισμός ασφαλείας που να σας προστατεύει από παραβίαση δεδομένων, κάθε μέθοδος είναι απλώς ένα πρόσθετο επίπεδο ασφάλειας που θα μπορούσε να αφαιρεθεί από μια επίθεση.

Ανέκδοτα, το πιο σύνθετο επίπεδο του μοντέλου OSI είναι το επίπεδο χρήστη/πολιτικού επιπέδου 8, επειδή η τεχνολογία βασίζεται στον άνθρωπο ή είναι απόηχος της ζωής μας και η ασφάλεια είναι κάτι που θέλουμε, αλλά πάντα στα πλεονεκτήματά μας, όχι κάποιου άλλου που μεταφέρει παντού από « μας» σε έναν μεμονωμένο άνθρωπο ή οργανισμό (όλα πρέπει να είναι ασφαλή αλλά όχι ασφαλή ταυτόχρονα) [65].

# Ανασκόπηση βιβλιογραφίας ανάλυσης πραγματικής περίπτωσης

## Η μελέτη περίπτωσης

### Tor επιλογές

Το Tor έχει πολλές επιλογές για τον τρόπο λειτουργίας, θα εξετάσουμε πώς να ρυθμίσετε έναν κόμβο Tor Relay και έναν διακομιστή κρυφής υπηρεσίας. Και οι δύο διαδικασίες απαιτούν το αρχείο torrc να προσαρμόζεται ανάλογα και βρίσκεται κάτω από: (μπορεί να είναι κρυφό)

* Linux: /etc/tor/torrc
* Windows: “path\_to\_tor“\Tor Browser\Browser\TorBrowser\Data\Tor\torcc
* macOS: ~/Library/Application Support/TorBrowser-Data/Tor/torrc

### torrc

Το torrc είναι ένα αρχείο διαμόρφωσης για την επεξεργασία του τρόπου συμπεριφοράς του Tor σε διάφορες υπηρεσίες, όπως η κρυφή υπηρεσία και ο κόμβος αναμετάδοσης. Η εσφαλμένη ρύθμιση παραμέτρων ή η παρακολούθηση οποιασδήποτε ασυνήθιστης πρακτικής αυτού του αρχείου μπορεί να οδηγήσει στο να διακυβεύσει την ασφάλειά του ο διακομιστής και να είναι ευάλωτος σε επιθέσεις. Οποιαδήποτε τροποποίηση στο ίδιο το αρχείο θα πρέπει να γίνει ενώ έχετε κλείσει το πρόγραμμα περιήγησης Tor, επειδή μπορεί να διαγράψει την τροποποίησή σας λόγω του χρόνου εκτέλεσης [66].

### Λειτουργία κόμβου ρελέ

Σύμφωνα με την τεκμηρίωση, υπάρχουν πολλές επιλογές ρελέ Tor για να διαλέξετε και μπορείτε να εκτελέσετε πολλές λειτουργίες του ρελέ ταυτόχρονα, αλλά όχι όλες. Για παράδειγμα, δεν μπορείτε να είστε ταυτόχρονα φύλακας εισόδου και κόμβος εξόδου [67].

Επίσης, πριν επιλέξουμε επίσης τη λειτουργία αναμετάδοσης, θα πρέπει να ελέγξουμε οποιαδήποτε νομική καταγγελία και προσέλκυση υπηρεσιών επιβολής του νόμου [68].

Για να το διαμορφώσουμε ως μεσαίο ρελέ ή κόμβο εξόδου, ακολουθούμε αυτούς τους κανόνες και γενικά πρέπει να έχουμε κάποιες δυνατότητες εύρους ζώνης καθώς και περισσότερα για αυτό εδώ [69] [70]:

• Χρησιμοποιήστε μια φυσική μηχανή ή/και εικονική ή πιθανή λύση (π.χ. DigitalOcean)

• Εγκαταστήστε το Linux ubuntu ή το kali linux και ενημερώστε το, εγκαταστήστε οποιοδήποτε repos για python και εγκαταστήστε το python εάν δεν είναι ήδη εγκατεστημένο.

• Προσθέστε repos εάν δεν μπορείτε να βρείτε το Tor στην εγκατάσταση sudo apt

• Βεβαιωθείτε ότι έχετε μια πολιτική τείχους προστασίας για τις θύρες και την προώθηση θύρας σε συσκευή δικτύου/δρομολογητή (NAT/PAT) για να επιτρέψετε την υποδοχή daemon που πρόκειται να ανοίξετε για Tor, π.χ. τη θύρα 4000 ή 9001.

• sudo nano /etc/tor/torrc

• χωρίς σχολιασμό και προσθέστε τις ακόλουθες γραμμές (αφαίρεση #) όπως απεικονίζεται στην Εικόνα 14

• Επίσης, μπορείτε να διαμορφώσετε το εύρος ζώνης οποιεσδήποτε περισσότερες επιλογές μπορείτε να βρείτε εδώ [67]

• sudo tor ή (systemctl ενεργοποίηση tor και systemctl start tor)

• Θα εμφανιστείτε στο δημόσιο μητρώο σε δύο ημέρες μετά την οικοδόμηση επιπέδου εμπιστοσύνης, γιατί μπορείτε να βρείτε περισσότερα σε αυτό το Σχήμα 15.

• Contratz απλά συνεισφέρετε σε αυτό το καταπληκτικό έργο με την προσθήκη ενός άλλου ρελέ κόμβου!

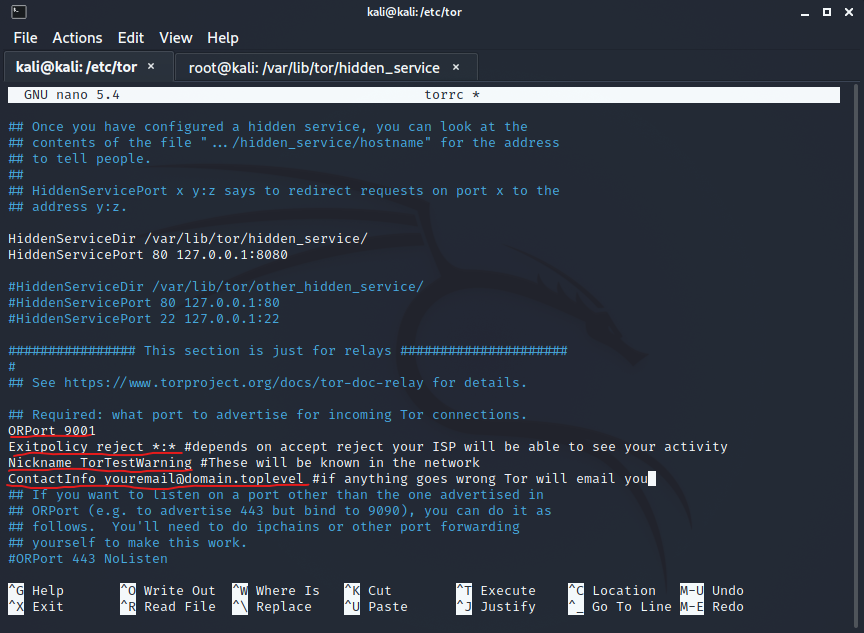


Figure 14 Tor relay config in torrc

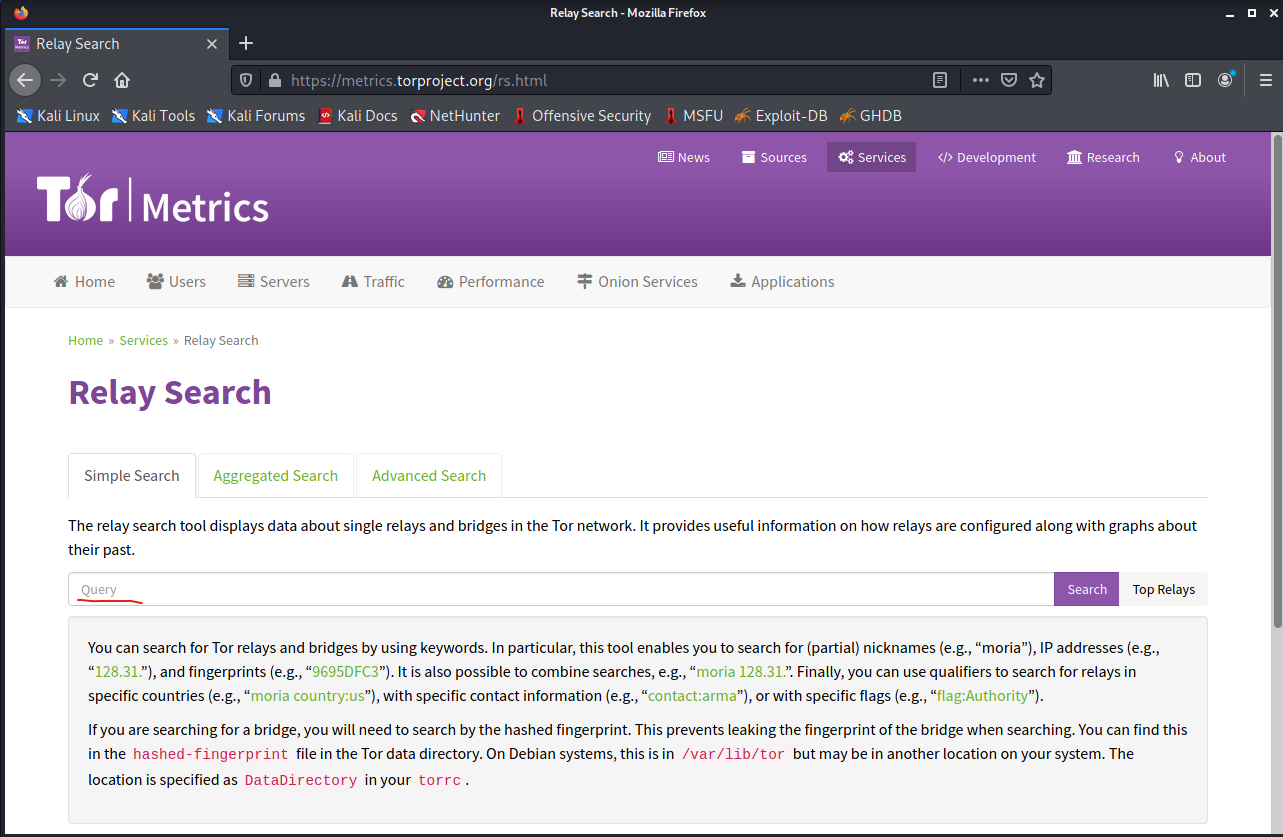


Figure 15 Tor metrics

### κρυφή υπηρεσία

Σύμφωνα με την τεκμηρίωση, πρέπει πρώτα να δημιουργήσετε έναν κατάλογο στον οποίο θα κατοικεί ο διακομιστής: [71]

• Είτε σε Φυσική μηχανή, εικονική μηχανή ή λύση cloud (π.χ. DigitalOcean)

• Εγκαταστήστε το Linux Ubuntu ή το kali Linux και ενημερώστε το, εγκαταστήστε οποιοδήποτε repos για python και εγκαταστήστε το python εάν δεν είναι ήδη εγκατεστημένο.

• Προσθέστε repos εάν δεν μπορείτε να βρείτε το Tor στην εγκατάσταση sudo apt

• mkdir tor\_service (οπουδήποτε)

• cd tor\_service

• python3-m http.server –bind 127.0.0.1 8080

o Αυτή η IP συνιστάται από την Tor προκειμένου να αποφευχθεί η ανακάλυψη από ορισμένες υπηρεσίες

• αγγίξτε index.html

• nano index.html

• <html><body> Δοκιμάστε την εφαρμογή κρυφής υπηρεσίας Tor</body></html>

• Σώσε το

• Ανοίξτε ένα πρόγραμμα περιήγησης Ιστού και πληκτρολογήστε url για τη θύρα "localhost:8080". Η ιστοσελίδα εκτελείται σε Python σε τοπικό μηχάνημα τώρα θέλουμε να τη φιλοξενήσουμε στο Tor

• Εγκαταστήστε το Tor και το Tor Browser

• ενημέρωση sudo apt

• sudo apt install -y tor tobrowser-launcher

• Whereis tor

• cd /etc/tor

• sudo nano torrc

• απέσυρε τις ακόλουθες γραμμές (αφαιρέστε το # και στις δύο και προσθέστε το 8080 ως θύρα) όπως απεικονίζεται στην Εικόνα 16

• σώσε το

• sudo tor

• Η κρυφή υπηρεσία εκτελείται για να τη δείτε στο πρόγραμμα περιήγησης Tor, χρειάζεστε τη διεύθυνση “.onion” και μπορείτε να τη λάβετε στο cd /var/lib/tor/hidden\_service ως χρήστης sudo su πριν μεταβείτε εκεί όπως φαίνεται στην Εικόνα 17.

• Αντιγράψτε τη διεύθυνση, επικολλήστε την μέσα στο Tor Browser και voila ο web server της Python φιλοξενείται στο Tor Network ως κρυφή υπηρεσία και όλοι όσοι έχουν αυτήν τη διεύθυνση από εδώ και στο εξής μπορούν να έχουν πρόσβαση στην Κρυφή Υπηρεσία σας!

Συνιστάται να έχετε τον δικό σας αποκλειστικό διακομιστή, όπως apache, tomcat ή οποιοδήποτε άλλο λογισμικό HTTP, επειδή πρόκειται να εκτελείτε μακροπρόθεσμα και να έχετε μεγάλη επισκεψιμότητα, πιθανότατα ο διακομιστής python ίσως να μην είναι κατάλληλος για τη δουλειά.

Τίποτα δεν είναι 100% ασφαλές, γι' αυτό προειδοποιήστε.

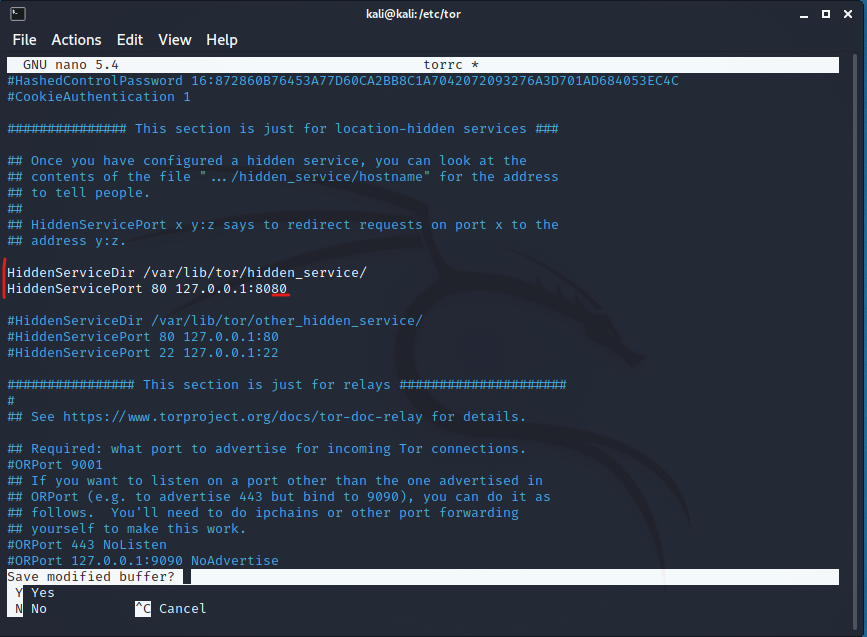


Figure 16 torrc for hidden services

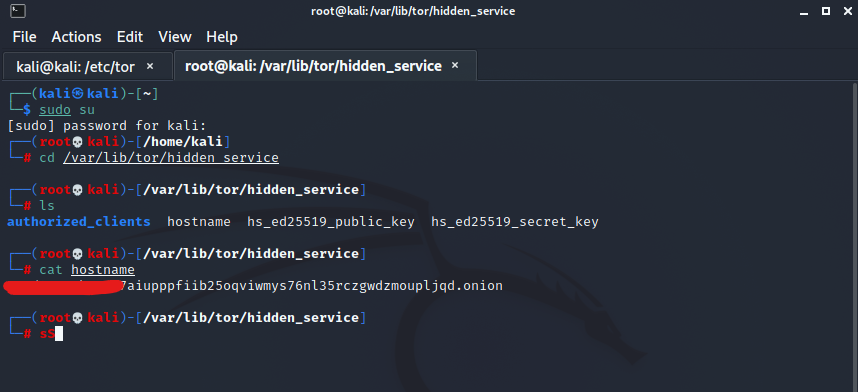


Figure 17 Find your .onion address

# References

|  |  |
| --- | --- |
| [1] | H. S. published, "A Brief History of Cryptography," redhat, 14 08 2013. [Online]. Available: https://access.redhat.com/blogs/766093/posts/1976023. [Accessed 11 11 2021]. |
| [2] | "Enigma machine - Wikipedia," [Online]. Available: https://en.wikipedia.org/wiki/Enigma\_machine. [Accessed 11 11 2021]. |
| [3] | "Alan Turing - Wikipedia," [Online]. Available: https://en.wikipedia.org/wiki/Alan\_Turing . [Accessed 11 11 2021]. |
| [4] | "Alan Turing," New Scientist, [Online]. Available: https://www.newscientist.com/people/alan-turing/?utm\_source=rakuten&utm\_medium=affiliate&utm\_campaign=3690980:Linkbux&utm\_content=10&ranMID=47192&ranEAID=wizKxmN8no4&ranSiteID=wizKxmN8no4-edVE.\_ke9k8oXwf4sksltw . [Accessed 11 11 2021]. |
| [5] | "A Brief History of the Internet," Usg.edu, [Online]. Available: https://www.usg.edu/galileo/skills/unit07/internet07\_02.phtml. [Accessed 11 11 2021]. |
| [6] | "ARPANET - Wikipedia," [Online]. Available: https://en.wikipedia.org/wiki/ARPANET. [Accessed 11 11 2021]. |
| [7] | "History of the Internet - Wikipedia," [Online]. Available: https://en.wikipedia.org/wiki/History\_of\_the\_Internet. [Accessed 11 11 2021]. |
| [8] | "Internet protocol suite - Wikipedia," [Online]. Available: https://en.wikipedia.org/wiki/Internet\_protocol\_suite. [Accessed 11 11 2021]. |
| [9] | "History of TCP/IP," scos, [Online]. Available: https://scos.training/history-of-tcp-ip/. [Accessed 11 11 2021]. |
| [10] | "IPv4 - Wikipedia," [Online]. Available: https://en.wikipedia.org/wiki/IPv4. [Accessed 11 11 2021]. |
| [11] | "IPsec - Wikipedia," [Online]. Available: https://en.wikipedia.org/wiki/IPsec. [Accessed 11 11 2021]. |
| [12] | "Introduction to Cisco IPsec Technology," Cisco, [Online]. Available: https://www.cisco.com/c/en/us/td/docs/net\_mgmt/vpn\_solutions\_center/2-0/ip\_security/provisioning/guide/IPsecPG1.html. [Accessed 11 11 2021]. |
| [13] | L. Center, "VPN History & The Future of VPN Technology," CactusVPN, [Online]. Available: https://www.cactusvpn.com/beginners-guide-to-vpn/vpn-history/. [Accessed 11 11 2021]. |
| [14] | "Tor (network) - Wikipedia," [Online]. Available: https://en.wikipedia.org/wiki/Tor\_(network). [Accessed 11 11 2021]. |
| [15] | "Internet service provider - Wikipedia," [Online]. Available: https://en.wikipedia.org/wiki/Internet\_service\_provider. [Accessed 11 11 2021]. |
| [16] | C. Press, " Hierarchical Network Design Overview (1.1) > Cisco Networking Academy Connecting Networks Companion Guide: Hierarchical Network Design," Cisco, [Online]. Available: https://www.ciscopress.com/articles/article.asp?p=2202410&seqNum=4. [Accessed 11 11 2021]. |
| [17] | "Understanding Using MPLS-Based Layer 2 and Layer 3 VPNs on EX Series Switches - TechLibrary," Juniper Networks, [Online]. Available: https://www.juniper.net/documentation/en\_US/junos/topics/concept/mpls-ex-series-vpn-layer2-layer3.html. [Accessed 11 11 2021]. |
| [18] | L. Cittadini, G. D. Battista and M. Patrignani, "MPLS Virtual Private Networks," [Online]. Available: http://sigcomm.org/education/ebook/SIGCOMMeBook2013v1\_chapter6.pdf. [Accessed 11 11 2021]. |
| [19] | "Public switched telephone network - Wikipedia," [Online]. Available: https://en.wikipedia.org/wiki/Public\_switched\_telephone\_network. [Accessed 11 11 2021]. |
| [20] | "PPPoE on Ethernet," Cisco, [Online]. Available: https://www.cisco.com/c/en/us/td/docs/ios/bbdsl/configuration/guide/bba\_ppoe\_enet.html. [Accessed 11 11 2021]. |
| [21] | "MPLS Point-to-Multipoint Traffic Engineering," Cisco, [Online]. Available: https://www.cisco.com/c/en/us/td/docs/ios/mpls/configuration/guide/12\_2sr/mp\_12\_2sr\_book/mp\_te\_p2mp.html. [Accessed 11 11 2021]. |
| [22] | "Introduction to Cisco MPLS VPN Technology," Cisco, [Online]. Available: https://www.cisco.com/c/en/us/td/docs/net\_mgmt/vpn\_solutions\_center/2-0/mpls/provisioning/guide/PGmpls1.html. [Accessed 11 11 2021]. |
| [23] | "Configuring Scalable Hub-and-Spoke MPLS VPNs," Cisco, [Online]. Available: https://www.cisco.com/c/en/us/td/docs/ios/mpls/configuration/guide/convert/mp\_l3\_vpns\_book/mp\_cfg\_hub\_spoke.html. [Accessed 11 11 2021]. |
| [24] | "MPLS/VPN Hub-and-spoke Topology," [Online]. Available: http://etutorials.org/Networking/MPLS+VPN+Architectures/Part+2+MPLS-based+Virtual+Private+Networks/Chapter+11.+Advanced+MPLS+VPN+Topologies/MPLS+VPN+Hub-and-spoke+Topology/. [Accessed 11 11 2021]. |
| [25] | "Leased Line Definition, Explanation, and Example," study-ccna, [Online]. Available: https://study-ccna.com/leased-line/. [Accessed 11 11 2021]. |
| [26] | "Leased line - Wikipedia," [Online]. Available: https://en.wikipedia.org/wiki/Leased\_line. [Accessed 11 11 2021]. |
| [27] | "Types of VPN and types of VPN Protocols," vpnoneclick, [Online]. Available: https://www.vpnoneclick.com/types-of-vpn-and-types-of-vpn-protocols/. [Accessed 11 11 2021]. |
| [28] | Y. Fujimoto, T. (JP) and T. Ohsawa, VIRTUAL PRIVATE NETWORK, U.S, 2004. |
| [29] | "Introduction to VPNs," networklessons, [Online]. Available: https://networklessons.com/cisco/ccna-routing-switching-icnd2-200-105/introduction-to-vpns. [Accessed 11 11 2021]. |
| [30] | "The Many Use-Cases of VPN: How a VPN Can be Useful," webhostingsecretrevealed, [Online]. Available: https://www.webhostingsecretrevealed.net/blog/security/how-a-vpn-can-be-useful/. [Accessed 11 11 2021]. |
| [31] | "An Overview of Enterprise VPN – Virtual Private Network," [Online]. Available: https://excitingip.com/780/an-introduction-for-enterprise-vpn-virtual-private-network/. [Accessed 11 11 2021]. |
| [32] | "Cisco Business VPN Overview and Best Practices," Cisco, [Online]. Available: https://www.cisco.com/c/en/us/support/docs/smb/routers/cisco-rv-series-small-business-routers/1399-tz-best-practices-vpn.html. [Accessed 11 11 2021]. |
| [33] | "Centralized vs Decentralized VPN, or VPN vs dVPN, Which Is the Better Protection for My Online Security and Privacy?," bitvpn, [Online]. Available: https://www.bitvpn.net/blog/centralized-vs-decentralized-vpn/. [Accessed 11 11 2021]. |
| [34] | "The Pros And Cons Of Using Tor Browser," [Online]. Available: https://www.noobslab.com/2020/01/the-pros-and-cons-of-using-tor-browser.html. [Accessed 11 11 2021]. |
| [35] | "Virtual private network - Wikipedia," [Online]. Available: https://en.wikipedia.org/wiki/Virtual\_private\_network. [Accessed 11 11 2021]. |
| [36] | "Cisco Site-to-Site VPN Technologies Comparison At-A-Glance," Cisco, [Online]. Available: https://www.cisco.com/c/dam/en/us/products/collateral/ios-nx-os-software/enterprise-class-teleworker-ect-solution/prod\_brochure0900aecd80582078.pdf. [Accessed 11 11 2021]. |
| [37] | S. Communications, "Finding the right VPN solution," [Online]. Available: https://sectraprodstorage01.blob.core.windows.net/communication-uploads/sites/4/2020/09/finding-the-right-vpn-solution.pdf#:~:text=As%20a%20rule%2C%20a%20traditional,the%20client%20and%20the%20server.. [Accessed 11 11 2021]. |
| [38] | "OpenVPN Tap vs Tun Mode," stackexchange, [Online]. Available: https://security.stackexchange.com/questions/46442/openvpn-tap-vs-tun-mode. [Accessed 11 11 2021]. |
| [39] | "Layer 3 VPNs User Guide for Routing Devices," Juniper, [Online]. Available: https://www.juniper.net/documentation/us/en/software/junos/vpn-l3/topics/topic-map/l3-vpns-overview.html. [Accessed 11 11 2021]. |
| [40] | "Web 1.0, Web 2.0 and Web 3.0 with their difference," geeksforgeeks, [Online]. Available: https://www.geeksforgeeks.org/web-1-0-web-2-0-and-web-3-0-with-their-difference/. [Accessed 11 11 2021]. |
| [41] | "Morgan Stanley’s Top Stock Picks for the $8 Trillion Metaverse Opportunity (Ep. 450), timestamp 3,41 - 14,44," YouTube, [Online]. Available: https://www.youtube.com/watch?v=g6BzocTEBig&list=PLiTVVRdEvpm6UuNLky1I58fy\_eavP5t92&index=20. [Accessed 11 11 2021]. |
| [42] | "THE BLOCKCHAIN BANDWIDTH INFRASTRUCTURE for web 3.0 (dVPN)," sentinel, [Online]. Available: https://sentinel.co/. [Accessed 11 11 2021]. |
| [43] | "Decentralized VPN: The Evolution of Tor?," hackernoon, [Online]. Available: https://hackernoon.com/decentralized-vpn-the-evolution-of-tor-hkv3uix. [Accessed 11 11 2021]. |
| [44] | "VPLS Overview," Juniper, [Online]. Available: https://www.juniper.net/documentation/en\_US/junos/topics/concept/vpls-security-overview.html. [Accessed 11 11 2021]. |
| [45] | "MPLS VPN Overview," Juniper, [Online]. Available: https://www.juniper.net/documentation/en\_US/junos/topics/concept/mpls-security-vpn-overview.html. [Accessed 11 11 2021]. |
| [46] | "Layer 2 Tunneling Protocol - Wikipedia," [Online]. Available: https://en.wikipedia.org/wiki/Layer\_2\_Tunneling\_Protocol. [Accessed 11 11 2021]. |
| [47] | "How TOR Works- Computerphile," YouTube, [Online]. Available: https://www.youtube.com/watch?v=QRYzre4bf7I. [Accessed 11 11 2021]. |
| [48] | R. Dingledine, N. Mathewson and P. Syverson, "Tor: The Second-Generation Onion Router," [Online]. Available: https://fermatslibrary.com/s/tor-the-second-generation-onion-router. [Accessed 11 11 2021]. |
| [49] | H. Zimmermann, "OSI Reference Model - The ISO Model of Architecture for Open Systems Interconnection," *in IEEE Transactions on Communications,* vol. 28, no. 4, pp. 425-432, April 1980. |
| [50] | B. Schneier, "Attacking Tor: how the NSA," the guardian, [Online]. Available: https://cyber-peace.org/wp-content/uploads/2013/06/Attacking-Tor\_-how-the-NSA-targets-users-online-anonymity-\_-World-news-\_-theguardian.pdf. [Accessed 11 11 2021]. |
| [51] | "TOR Hidden Services - Computerphile," YouTube, [Online]. Available: https://www.youtube.com/watch?v=lVcbq\_a5N9I. [Accessed 11 11 2021]. |
| [52] | M. Perry, "This is What a Tor Supporter Looks Like: Edward Snowden | Tor Blog," 2015. |
| [53] | L. Diana, T. Huete and R.-M. Antonio, "Tor Hidden Services: a systematic literature review," *MDPI,* vol. 1, no. 3, pp. 496-518, 2021. |
| [54] | "Tor Project. Tor Design Documents," 2021. |
| [55] | "Someone Is Running Hundreds of Malicious Servers on the Tor Network and Might Be De-Anonymizing Users," gizmodo, [Online]. Available: https://gizmodo.com/someone-is-running-hundreds-of-malicious-servers-on-the-1848156630. [Accessed 05 12 2021]. |
| [56] | "Meta Delays Offering End-to-End Encryption by Default Until 2023: Here's Why," [Online]. Available: https://www.makeuseof.com/meta-delays-end-to-end-encryption-until-2023/?utm\_source=MUO-FB-P&utm\_medium=Social-Distribution&utm\_campaign=MUO-FB-P&fbclid=IwAR3oGMRuVTXgFJvcsx\_AIiVC53D2Gvxwp5Tj5RhgB83Q1mkr7esLuVcBNLc. [Accessed 11 11 2021]. |
| [57] | "OpenVPN - Wikipedia," [Online]. Available: https://en.wikipedia.org/wiki/OpenVPN. [Accessed 11 11 2021]. |
| [58] | "OpenVPN – Pros and Cons," [Online]. Available: https://bobcares.com/blog/openvpn-pros-and-cons/. [Accessed 11 11 2021]. |
| [59] | "Is OpenVPN end to end encryption?," [Online]. Available: https://theknowledgeburrow.com/is-openvpn-end-to-end-encryption/. [Accessed 11 11 2021]. |
| [60] | "6 Advantages and Disadvantages of OpenVPN | Limitations & Benefits of OpenVPN," [Online]. Available: https://www.hitechwhizz.com/2020/08/6-advantages-and-disadvantages-drawbacks-benefits-of-openvpn.html. [Accessed 11 11 2021]. |
| [61] | "Advantages and disadvantages of tor browser," [Online]. Available: https://www.itrelease.com/2021/05/advantages-and-disadvantages-of-tor-browser/. [Accessed 11 11 2021]. |
| [62] | "The pros and cons of the Tor browser," [Online]. Available: https://broadbanddeals.co.uk/guides/the-pros-and-cons-of-the-tor-browser/. [Accessed 11 11 2021]. |
| [63] | "Blockchain-Enabled End-to-End Encryption for Instant Messaging Applications," Cornell Universiy, [Online]. Available: https://arxiv.org/abs/2104.08494. [Accessed 11 11 2021]. |
| [64] | "Using Blockchain to Facilitate End-to-End Encryption (E2EE)," hackernoon, [Online]. Available: https://hackernoon.com/using-blockchain-to-facilitate-end-to-end-encryption-e2ee-b1r221q. [Accessed 11 11 2021]. |
| [65] | "Layer 8," computerhope, [Online]. Available: https://www.computerhope.com/jargon/l/layer8.htm. [Accessed 11 11 2021]. |
| [66] | "I'm supposed to "edit my torrc". What does that mean?," torproject, [Online]. Available: https://support.torproject.org/tbb/tbb-editing-torrc/. [Accessed 11 11 2021]. |
| [67] | "Tor Project | Technical Setup," torproject, [Online]. Available: https://community.torproject.org/relay/setup/. [Accessed 11 11 2021]. |
| [68] | "What is a Tor Relay?," eff, [Online]. Available: https://www.eff.org/pages/what-tor-relay. [Accessed 11 11 2021]. |
| [69] | "Relay Operations," torproject, [Online]. Available: https://community.torproject.org/relay/. [Accessed 11 11 2021]. |
| [70] | "TorRelayGuide," torproject, [Online]. Available: https://gitlab.torproject.org/legacy/trac/-/wikis/TorRelayGuide. [Accessed 11 11 2021]. |
| [71] | "Tor Project | Onion Services," torproject, [Online]. Available: https://community.torproject.org/onion-services/. [Accessed 11 11 2021]. |
| [72] | "Sample Configuration Using the ip nat outside source static Command," Cisco, [Online]. Available: https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/13773-2.html. [Accessed 11 11 2021]. |
| [73] | "Network Address Translation (NAT) FAQ," Cisco, [Online]. Available: https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/26704-nat-faq-00.html. [Accessed 11 11 2021]. |
| [74] | "Cryptanalysiss Software Attack," OWASP Foundation, [Online]. Available: https://owasp.org/www-community/attacks/Cryptanalysis. [Accessed 11 11 2021]. |
| [75] | "Cisco three-layer hierarchical model," Study CCNA, [Online]. Available: https://study-ccna.com/cisco-three-layer-hierarchical-model/ . [Accessed 11 11 2021]. |
| [76] | "Hierarchical internetworking model - Wikipedia," [Online]. Available: https://en.wikipedia.org/wiki/Hierarchical\_internetworking\_model. [Accessed 11 11 2021]. |
| [77] | "Backhaul (telecommunications) - Wikipedia," [Online]. Available: https://en.wikipedia.org/wiki/Backhaul\_(telecommunications). [Accessed 11 11 2021]. |
| [78] | "Difference Between ISDN BRI and PRI," [Online]. Available: http://www.differencebetween.net/technology/communication-technology/difference-between-isdn-bri-and-pri/. [Accessed 11 11 2021]. |
| [79] | "Why can't a Tor node simultaneously be a guard and an exit node?," security stackexchange, [Online]. Available: https://security.stackexchange.com/questions/200568/why-cant-a-tor-node-simultaneously-be-a-guard-and-an-exit-node. [Accessed 11 11 2021]. |
| [80] | R. Dingledine, N. Mathewson and P. Syverson, "Tor: The Second-Generation Onion Router," *Naval Research Lab,* 2004. |

# Appendix

## Glossary

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Agnostic | Δεν εξαρτάται από το περιεχόμενο, π.χ., χωρίς έντυπη κωδικοποίηση |
| Abstraction | Μια άποψη υψηλού επιπέδου των πραγμάτων από την οπτική γωνία του τελικού καταναλωτή χωρίς να γνωρίζει πάρα πολλά για τους υποκείμενους μηχανισμούς του, αλλά εξακολουθεί να μπορεί να το χρησιμοποιήσει. |
| LAN | Ένα ιδιωτικό τοπικό δίκτυο συνήθως μικρό εύρος λογικής (επικάλυψης) όχι σε φυσικό απαραίτητο. |
| VLAN | Εικονικά πολλαπλά δίκτυα στον ίδιο διακόπτη. Δημιουργεί έναν τομέα μετάδοσης. Διαχωρισμός ομάδων περιοχών LAN. |
| DMVPN | Πρωτόκολλο Cisco για δυναμική ρύθμιση πολλαπλών VPN |
| Socket Secure (SOCKS/Proxy) | είναι μια τεχνολογία που δημιουργήθηκε στις αρχές της δεκαετίας του 1990 και χρησιμοποιεί διακομιστές μεσολάβησης για την αναμετάδοση της κυκλοφορίας μεταξύ δικτύων ή συστημάτων (π.χ. διαμορφώνετε για την αποστολή και λήψη κίνησης σε υπολογιστή ένα διακομιστή μεσολάβησης: Θύρα + διαπιστευτήρια, εάν υπάρχουν, αυτό μπορεί να ισχύει σε επίπεδο εφαρμογής που σημαίνει συγκεκριμένη εφαρμογή απαιτεί διακομιστή μεσολάβησης για την επικοινωνία ή επίπεδο λειτουργικού συστήματος που διαμορφώνετε έναν διακομιστή μεσολάβησης/κάλτσες και η επισκεψιμότητά σας διέρχεται μέσω του διακομιστή μεσολάβησης ως ρελέ αντί να αποστέλλεται από τον υπολογιστή σας απευθείας στην υπηρεσία Target) |
| TUN/TAP | Προγράμματα οδήγησης πυρήνα/Εικονικοί προσαρμογείς δικτύου/διεπαφές που προσομοιώνουν φυσικές συνδέσεις π.χ. ethernet για μεταφορά δεδομένων, ότι βρίσκονται σε εφαρμογή χώρου χρήστη που δημιουργήθηκε εικονικά και παρέχουν λήψη και μετάδοση πακέτων. Οι πελάτες λογισμικού VPN μπορούν να αλληλεπιδράσουν με αυτές ως συσκευές P2P ή ethernet προκειμένου να περάσουν ή να προωθήσουν επισκεψιμότητα από το πρόγραμμα χώρου χρήστη (πελάτης VPN) στο φυσικό δίκτυο. L3/L2 που χρησιμοποιείται από VPN. |
| Peer-to-peer | Ένα δίκτυο πλέγματος με οποιονδήποτε κόμβο συνδεδεμένο μεταξύ τους. |
| Transparency | Δεν είναι ξεκάθαρο τι συμβαίνει στο παρασκήνιο. |
| Internet | Συνδέοντας υπολογιστές μαζί σε όλο τον κόσμο σχηματίζοντας ένα γράφημα/δίκτυο. |
| Web | Επίπεδο λογισμικού (Ένας τύπος λογισμικού) που εκτελείται στο φυσικό Διαδίκτυο για την κοινή χρήση πληροφοριών. Άλλοι τύποι λογισμικού είναι η ανταλλαγή email, το FTP |
| Deep web | Περιεχόμενο πίσω από κωδικούς πρόσβασης που δεν έχει ευρετηριαστεί από μηχανή αναζήτησης (π.χ. ιδιωτικό προφίλ στο Facebook). Είναι το κανονικό τμήμα Web χωρίς ευρετήριο. |
| Dark web | Ένα αντίγραφο του Ιστού αλλά με διαφορετική γλώσσα ενσωματωμένη για να κάνει τα ίδια πράγματα με τον ιστό, επομένως χρειάζεστε κατάλληλο πρόγραμμα περιήγησης για να ξέρετε πώς να μιλάτε (ζητήστε πληροφορίες για να λάβετε από αυτές τις σελίδες) σε αυτές τις σελίδες. Μυστικός κωδικός συνομιλιών. |
| FTP | Το πρωτόκολλο μεταφοράς αρχείων είναι μια υπηρεσία/εφαρμογή/λογισμικό περισσότερο από ένα πρωτόκολλο (ένα λογισμικό που υλοποιεί ένα/τα πρωτόκολλο) (γενικά αυτό σχετίζεται με όλες τις υπηρεσίες του επιπέδου 7) που στέλνετε αρχεία σε άλλους υπολογιστές αντί να κάνετε λήψη ιστοσελίδων από αυτούς χρησιμοποιώντας HTTP |
| HTTP | Ένα κείμενο με συνδέσμους (υπερκείμενο - ανακατεύθυνση). Ένας τρόπος για να δείτε ιστοσελίδες σε έναν τομέα (διεύθυνση IP)/URL άλλοι τρόποι περιλαμβάνουν το FTP. |
| Symmetric NAT | Όλα τα αιτήματα από την ίδια εσωτερική IP και θύρα προς μια συγκεκριμένη IP προορισμού και θύρα (υπηρεσία στόχου) αντιστοιχίζονται στην ίδια μοναδική διεύθυνση IP εξωτερικής πηγής. Εάν ο ίδιος εσωτερικός κεντρικός υπολογιστής στέλνει ένα πακέτο ακόμη και με την ίδια διεύθυνση πηγής και θύρα αλλά σε διαφορετικό προορισμό, χρησιμοποιείται διαφορετική αντιστοίχιση. Μόνο ένας εξωτερικός κεντρικός υπολογιστής που λαμβάνει ένα πακέτο από έναν εσωτερικό κεντρικό υπολογιστή μπορεί να στείλει ένα πακέτο πίσω. [72] [73] |
| Cipher | Ο κρυπτογράφηση είναι ένας αλγόριθμος που χρησιμοποιείται για κρυπτογράφηση ή αποκρυπτογράφηση. |
| Cryptanalysis | Η κρυπτανάλυση είναι μια διαδικασία εύρεσης αδυναμιών σε κρυπτογραφικούς αλγόριθμους και χρήσης αυτών των αδυναμιών για την αποκρυπτογράφηση του κρυπτογραφημένου κειμένου χωρίς να γνωρίζουμε το μυστικό κλειδί [74] |
| Internetwork | Δίκτυο δικτύων γνωστό και ως Διαδίκτυο |
| CIA | Εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα |
| Key exchange (e.g., Diffie-hellman) | Το Diffie-Hellman είναι ένας τρόπος δημιουργίας ενός κοινού μυστικού μεταξύ δύο ανθρώπων με τέτοιο τρόπο ώστε το μυστικό να μην μπορεί να φανεί παρατηρώντας την επικοινωνία. Δεν μοιράζεστε πληροφορίες κατά την ανταλλαγή κλειδιών, δημιουργείτε ένα κλειδί μαζί. Εν ολίγοις, είναι μια μέθοδος ασύμμετρης κρυπτογράφησης που στέλνει το νέο κοινόχρηστο μυστικό κλειδί (συμμετρικά κρυπτογραφημένο) το οποίο είναι πιο ελαφρύ για την επιβάρυνση της κυκλοφορίας σε σύγκριση με την κρυπτογράφηση δεδομένων ασύμμετρων κλειδιών για ασφαλή κοινή χρήση σε ανοιχτό κοινό (διαδίκτυο). |
| Blockchain | Εποχή Web 3.0 όπου τα πάντα είναι αποκεντρωμένα σε ένα mesh δίκτυο p2p και κάθε ενέργεια έχει μια συναλλαγή είτε μεταφέροντας κάτι είτε δημιουργώντας μια εφαρμογή Ιστού και τοποθετείτε στο blockchain. Αυτή η τεχνολογία είναι διαφανής από την άποψη του κώδικα ως ανοιχτού κώδικα, αλλά όχι διαφανής για τις συναλλαγές της. Χρησιμοποιεί ψηφιακές υπογραφές που βασίζονται σε ασύμμετρη κρυπτογραφία κλειδιού και η ακεραιότητά του εξαρτάται από το κρυπτοσύστημα με το κλειδί. Πολύ βολικό για σκοπούς ελέγχου ταυτότητας και άμυνας από επιθέσεις ασφαλείας, δηλαδή, δεν μπορεί να διεισδύσει μόνο σε κίνδυνο ενός μηχανήματος. [64] |
| Asymmetric encryption | Περισσότερο υπολογιστικά έντονο από το κοινό συμμετρικό κλειδί. Κρυπτογράφηση δημόσιου ιδιωτικού κλειδιού. Το δημόσιο κλειδί μπορεί να κρυπτογραφήσει/υπογράψει/επικυρώσει ένα μήνυμα και το ιδιωτικό μπορεί να το αποκρυπτογραφήσει/αποκρυπτογραφήσει/επαληθεύσει. Χρησιμοποιείται επίσης στην ψηφιακή υπογραφή/δακτυλικό αποτύπωμα για τον έλεγχο ταυτότητας του αποστολέα με ή χωρίς πιστοποιητικό δημόσιας γνωστής γνησιότητας που είναι αποθηκευμένο σε ειδικό διακομιστή. |
| Private (signing key) and public (verification) key | Συνδέονται μαθηματικά. Το κοινό είναι ορατό από άλλους και το ιδιωτικό προορίζεται να είναι μόνο στην κατοχή του ιδιοκτήτη/των. Το ιδιωτικό αποκρυπτογραφεί το περιεχόμενο δεδομένων του κοινού. |
| Certificate | Ένας μετρητής επιπέδου εμπιστοσύνης της υπογραφής. Πιστοποίηση δακτυλικού αποτυπώματος που σημαίνει ότι έχει εγκριθεί από άλλα άτομα ή αξιόπιστο αποκλειστικό ιστότοπο. Μια υπογραφή (σήμα) λαμβάνει επίπεδο «εμπιστοσύνης» με πιστοποιητικό, δεν χρειάζεται, αν και για οποιαδήποτε πραγματική αποκρυπτογράφηση μόνο για αναγνώριση/γνησιότητα της πηγής για το επίπεδο εμπιστοσύνης που έχει εγκριθεί από άλλους ή μια αρχή. |
| Sign/Digital Signature | Οποιοσδήποτε μπορεί να κρυπτογραφήσει ένα μήνυμα χρησιμοποιώντας δημόσιο κλειδί και να το στείλει κάπου, η αποκρυπτογράφηση πραγματοποιείται μόνο σε όσους έχουν πρόσβαση στο ιδιωτικό κλειδί που δημιούργησε αυτό το δημόσιο κλειδί. Εάν το μήνυμα είναι απλώς κρυπτογραφημένο χωρίς υπογραφή, τότε μπορείτε ακόμα να διαβάσετε το μήνυμα (με αποκρυπτογράφηση ιδιωτικού κλειδιού), αλλά δεν μπορείτε πραγματικά να πείτε ποιος πραγματικά έστειλε αυτό το μήνυμα παρά το γεγονός ότι θα μπορούσατε να το λάβετε στα εισερχόμενά σας email από έναν γνωστό διεύθυνση που δεν σημαίνει ότι είναι το πραγματικό άτομο που τη στέλνει.  Ένα σημάδι είναι μια διαφορετική προσέγγιση από την κρυπτογράφηση  Το "de-Sign" δεν χρειάζεται κλειδί αποκρυπτογράφησης για να είναι γνωστό.  Όταν υπογράφετε ένα μήνυμα (κάτι που συμβαίνει με το ιδιωτικό σας κλειδί), δημιουργείτε ένα κλειδί με αριθμούς που φαίνονται παράξενα (το κείμενο είναι κρυπτογραφημένο βασικά μόνο στο τμήμα της υπογραφής και όχι στο πραγματικό μήνυμα που θέλετε να μεταφέρετε) αλλά δεν λέει πουθενά το όνομά σας μόνο αριθμούς , τώρα οποιοσδήποτε έχει το δημόσιο κλειδί σας (αυτό το ιδιωτικό κλειδί που έλαβε αυτό το δημόσιο κλειδί μπορεί να κρυπτογραφήσει/αποκρυπτογραφήσει/υπογράψει/επικυρώσει) χωρίς να απαιτείται κωδικός πρόσβασης, μπορεί να «αποκρυπτογραφήσει/απυπογράψει» την υπογραφή και να αποκαλύψει το όνομά σας. Εάν πραγματοποιηθούν και τα δύο, π.χ. Κρυπτογράφηση με υπογραφή, τότε για να το διαβάσετε χρειάζεστε το ιδιωτικό κλειδί και επίσης αποκαλύπτεται το "ποιος" το υπέγραψε (που είναι ο πραγματικός αποστολέας).  Για ένα σύντομο παράδειγμα, θέλετε να στείλετε ένα μυστικό μήνυμα στο άτομο Α, είστε το άτομο Β και τα δύο έχουν ασύμμετρα κλειδιά, αλλά δεν έχετε το ιδιωτικό κλειδί του άλλου μόνο δημόσιο. Κρυπτογραφείτε το Μήνυμα με το δημόσιο κλειδί του ατόμου Α, ώστε να μπορεί να το αποκρυπτογραφήσει μόνο αυτός/αυτή και μαζί με εσάς να το υπογράψετε με το ιδιωτικό σας κλειδί (Άτομο Β). Στη συνέχεια, το άτομο Α πρέπει να έχει το ιδιωτικό του κλειδί και το δημόσιο κλειδί σας, ώστε τόσο το κρυπτογραφημένο μήνυμα που του παραπέμπει να μπορεί να αποκαλυφθεί ως η μακριά πλευρά με το όνομά σας που αποκαλύπτεται «αποκρυπτογραφώντας» την υπογραφή σας με το δημόσιο κλειδί σας (Ατομικό Β).    Η υπογραφή είναι μια λειτουργία που παίρνει ένα μήνυμα και ένα ιδιωτικό κλειδί και δημιουργεί μια ψηφιακή υπογραφή Το μήνυμα θα μπορούσε να είναι κενό, αλλά αυτό είναι άσκοπο.  Οποιοσδήποτε μπορεί να χρησιμοποιήσει το δημόσιο κλειδί για να επαληθεύσει μια ψηφιακή υπογραφή: |

1. From traffic perspective not actual code implementation because they are open-source most of them. [↑](#footnote-ref-2)
2. Συνήθως, η λήψη του προγράμματος-πελάτη λογισμικού γίνεται με αυτόματη ανακατεύθυνση κατά τη σύνδεση σε μια πύλη «VPN». [↑](#footnote-ref-3)
3. Η κρυπτογράφηση από άκρο σε άκρο εξαρτάται εάν ο κεντρικός υπολογιστής που συνδέεται σε ένα απομακρυσμένο δίκτυο ή έναν κεντρικό υπολογιστή και αυτό το δίκτυο ή ο κεντρικός υπολογιστής (απομακρυσμένος) εφαρμόζει οποιαδήποτε κρυπτογράφηση στη ληφθείσα κίνηση ή στην υπηρεσία προορισμού εκτός του κόμβου εξόδου VPN χρησιμοποιεί κρυπτογράφηση , επομένως ο χρήστης πρέπει να γνωρίζει σχετικά με την εφαρμογή τεχνολογίας στο Επίπεδο 3 (π.χ. IPsec) ή/και στο Επίπεδο 7 (π.χ. https) [↑](#footnote-ref-4)
4. Αξίζει να σημειωθεί ότι οι συσκευές TUN/TAP χρησιμοποιούνται μόνο από συγκεκριμένα πρωτόκολλα VPN (όπως το OpenVPN και άλλα) αλλά όχι από ορισμένα όπως το IKEv2/IPsec αλλά και πάλι μπορείτε να εφαρμόσετε την ιδέα του TUN/TAP είτε με L2 IPsec είτε με L3 IPsec π.χ. , L2TP/IPsec ή IKEv2/IPsec [↑](#footnote-ref-5)
5. Η έκδοση v2,3 αντιπροσωπεύει το επίπεδο ασφάλειας του αλγορίθμου κρυπτογράφησης HS, δεν θέλουν πολλά άτομα να έχουν πρόσβαση σε ένα V2 (κίνδυνος ανωνυμοποίησης) [↑](#footnote-ref-6)
6. Τα ρελέ εξόδου είναι γνωστά στο κοινό [↑](#footnote-ref-7)
7. εκτός εάν χρησιμοποιείτε VPN στη λειτουργία κόμβου εξόδου για εξερχόμενη κίνηση; [↑](#footnote-ref-8)
8. Εγκαθιστάτε την εφαρμογή διακομιστή και τον πελάτη διαμορφώνοντάς τα με τους δικούς σας κανόνες. [↑](#footnote-ref-9)
9. Η κίνηση εκτός της σήραγγας κρυπτογραφείται μόνο εάν τα πρωτόκολλα που χρησιμοποιούνται βασίζονται σε κρυπτογράφηση (δηλαδή SSH, pop3 κ.λπ.) και εάν η απομακρυσμένη πρόσβασή της (host-to-host) τότε είναι δυνατή, δεν υπάρχει E2EE, εκτός εάν η στοχευόμενη υπηρεσία κεντρικού υπολογιστή/υποδοχή η σύνδεση με την οποία προωθείται η κίνηση χρησιμοποιεί κρυπτογράφηση (π.χ., εάν ο ιστότοπος που επισκέπτεστε είναι HTTP, ο κόμβος VPN τελικής εξόδου δεν θα έχει κρυπτογράφηση όπως αναφέρεται στον ιστότοπο από κεντρικό υπολογιστή σε ιστότοπο στόχο). [↑](#footnote-ref-10)
10. Κάνει σχεδόν αδύνατη την επίθεση ενός Man in the Middle από την αποκρυπτογράφηση όλων των πακέτων δεδομένων που συγκεντρώθηκαν μεταξύ διαφορετικών περιόδων/περιόδων σύνδεσης, επειδή πρέπει να βρίσκει κάθε φορά το νέο κρυπτοκλειδί για αποκρυπτογράφηση. [↑](#footnote-ref-11)
11. Το πραγματικό ωφέλιμο φορτίο δεδομένων για το Επίπεδο Εφαρμογής στο μοντέλο TCP/IP δεν είναι κρυπτογραφημένο από το Tor, επομένως ο κόμβος εξόδου θα αφαιρέσει το τελικό στρώμα του κρυπτογραφημένου πακέτου του δικτύου Tor, αλλά το Επίπεδο Εφαρμογής θα είναι μόνο του από τώρα και στο εξής, ανάλογα με την υπηρεσία που θα ο χρήστης ξεκίνησε για να κάνει επαφή/πρίζα με/socket. [↑](#footnote-ref-12)
12. Και πάλι, ο χρήστης πρέπει να γνωρίζει την τελική υπηρεσία στόχο που θέλει να φτάσει (http, https) στην εξερχόμενη διεπαφή του χρήστη θα κρυπτογραφήσει την επισκεψιμότητα επειδή περνά από το πρόγραμμα περιήγησης στη διεπαφή ως εισερχόμενη (μοντέλο OSI ενθυλάκωσης από πάνω προς τα κάτω) και επίσης Η επισκεψιμότητα θα λαμβάνει επιπλέον επίπεδα κρυπτογράφησης μέσα στο δίκτυο Tor, αλλά στον τελικό κόμβο εξόδου το πραγματικό επίπεδο επιπέδου Δεδομένων Εφαρμογής θα είναι από μόνο του. [↑](#footnote-ref-13)
13. Μια επίθεση σε κόμβο φύλαξης και/ή κόμβο εξόδου θα μπορούσε να αποδειχθεί μοιραία για την ανωνυμοποίηση του χρήστη. [↑](#footnote-ref-14)