**Όνομα:** _____ **Ημερομηνία:** _____ **Βαθμολογία:** _____

## ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 10

# Συχνές ερωτήσεις για τα VPN

*Διαδραστικό φύλλο εργασίας και οδηγός μελέτης*

Με βάση: τον Οδηγό του VPN.com για τα VPN: **https://www.vpn.com/el/vpn/**

Φύλλο εργασίας «Τι είναι ένα VPN»

# Σημείο ελέγχου 10: Συχνές ερωτήσεις για τα VPN – βασικό επίπεδο (Μέρος Α)

Εξέτασε τις πιο συχνές ερωτήσεις και απαντήσεις που έχουν οι υποψήφιοι πελάτες για τη χρήση εικονικών ιδιωτικών δικτύων.

### Q1: Τι είναι ένα VPN και πώς λειτουργεί;

Ένα εικονικό ιδιωτικό δίκτυο (VPN) κρυπτογραφεί τη σύνδεσή σου στο διαδίκτυο και δρομολογεί την κίνησή σου μέσω ενός ασφαλούς απομακρυσμένου διακομιστή. Έτσι κρύβεται η δημόσια διεύθυνση IP σου και περιορίζεται τι μπορούν να δουν για την κίνηση που περνά από τη σήραγγα VPN οι παρατηρητές του τοπικού δικτύου και ο ISP σου.

### Q2: Γιατί να χρησιμοποιήσω VPN;

Ένα VPN προστατεύει την ψηφιακή σου ιδιωτικότητα, ασφαλίζει τη σύνδεσή σου σε δημόσια δίκτυα Wi-Fi (όπως σε καφετέριες ή αεροδρόμια), μπορεί να μειώσει τον περιορισμό ταχύτητας βάσει δραστηριότητας όταν ο ISP δεν μπορεί να αναγνωρίσει τον τύπο της κρυπτογραφημένης κίνησης, παρακάμπτει γεωγραφικούς περιορισμούς για πρόσβαση σε παγκόσμιο περιεχόμενο και βοηθά στην ασφάλεια των πόρων απομακρυσμένης εργασίας.

### Q3: Με κάνει ένα VPN εντελώς ανώνυμο στο διαδίκτυο;

Όχι. Ενώ ένα VPN κρύβει τη διεύθυνση IP σου και κρυπτογραφεί την κίνηση, μπορείς ακόμη να παρακολουθείσαι μέσω cookies του προγράμματος περιήγησης, ενεργών λογαριασμών (όπως Google ή Facebook), fingerprinting του προγράμματος περιήγησης ή αν ο πάροχος του VPN καταγράφει τα δεδομένα σου.

### Q4: Θα επιβραδύνει ένα VPN την ταχύτητα του διαδικτύου μου;

Ναι, ελαφρώς. Η διαδικασία κρυπτογράφησης και η φυσική απόσταση από τον διακομιστή VPN προσθέτουν καθυστέρηση και επιβάρυνση. Η επίδραση διαφέρει ανάλογα με τον πάροχο, το πρωτόκολλο, την απόσταση από τον διακομιστή, τη συσκευή και τις συνθήκες του δικτύου.

### Q5: Είναι νόμιμη η χρήση VPN;

Η χρήση VPN είναι νόμιμη σε πολλές χώρες, αλλά ορισμένες δικαιοδοσίες περιορίζουν, ρυθμίζουν ή αποκλείουν υπηρεσίες VPN. Οι χρήστες πρέπει να επαληθεύουν τους ισχύοντες τοπικούς νόμους πριν από τη χρήση. Για περισσότερες λεπτομέρειες, συμβουλεύσου τους οδηγούς νομιμότητας στο VPN.com.

# Σημείο ελέγχου 10: Συχνές ερωτήσεις για τα VPN – βασικό επίπεδο (Μέρος Β)

Εξέτασε τις πιο συχνές ερωτήσεις και απαντήσεις που έχουν οι υποψήφιοι πελάτες για τη χρήση εικονικών ιδιωτικών δικτύων.

### Q6: Μπορώ να χρησιμοποιήσω δωρεάν VPN;

Τα δωρεάν VPN μπορεί να βασίζονται σε διαφημίσεις, περιορισμένες λειτουργίες, αναλύσεις χρήσης, όρια δεδομένων ή άλλα μοντέλα εσόδων. Οι χρήστες πρέπει να ελέγχουν την πολιτική απορρήτου, την ιδιοκτησία, τους ελέγχους και το επιχειρηματικό μοντέλο του παρόχου πριν από τη χρήση.

### Q7: Τι είναι η πολιτική «no-logs»;

Η πολιτική μη τήρησης αρχείων καταγραφής περιγράφει ποια δεδομένα δραστηριότητας και σύνδεσης δηλώνει ο πάροχος ότι δεν διατηρεί. Η ακριβής έκταση διαφέρει, γι' αυτό οι αναγνώστες πρέπει να ελέγχουν την πολιτική και τα ευρήματα ανεξάρτητων ελέγχων.

### Q8: Πώς επιλέγω το καλύτερο VPN;

Αναζήτησε ελεγμένες πολιτικές μη καταγραφής, ισχυρά πρωτόκολλα (WireGuard, OpenVPN), ασφαλείς τοποθεσίες διακομιστών, γρήγορες ταχύτητες, διακομιστές μόνο RAM, λειτουργία kill switch και δικαιοδοσία εκτός συμμαχιών ανταλλαγής πληροφοριών (όπως οι 5/9/14 Eyes).

### Q9: Μπορώ να χρησιμοποιήσω VPN στο κινητό και στην έξυπνη τηλεόρασή μου;

Ναι. Οι σύγχρονοι πάροχοι VPN προσφέρουν ειδικές εφαρμογές για iOS, Android, macOS, Windows, Linux και έξυπνες τηλεοράσεις, καθώς και ρυθμίσεις router για την προστασία όλων των συσκευών του οικιακού σου δικτύου.

### Q10: Τι είναι ο Kill Switch;

Ο Kill Switch είναι μια λειτουργία ασφαλείας που αποσυνδέει αυτόματα τη συσκευή σου από το διαδίκτυο αν διακοπεί η σύνδεση VPN. Έτσι αποτρέπεται η διαρροή των μη κρυπτογραφημένων δεδομένων ή της πραγματικής διεύθυνσης IP σου.

# Σημείο ελέγχου 10: Συχνές ερωτήσεις για τα VPN – προχωρημένο επίπεδο (Μέρος C)

Εξερεύνησε τεχνικές και δομικές πτυχές των εικονικών ιδιωτικών δικτύων και των ασφαλών πρωτοκόλλων τούνελ.

### Q1: Ποια είναι η διαφορά μεταξύ WireGuard, OpenVPN και IKEv2;

Το WireGuard είναι ένα σύγχρονο, ελαφρύ πρωτόκολλο (μόλις ~4.000 γραμμές κώδικα) που προσφέρει γρήγορες ταχύτητες και σύντομους χρόνους σύνδεσης. Το OpenVPN είναι ένα εξαιρετικά ασφαλές, δοκιμασμένο στην πράξη πρωτόκολλο ανοιχτού κώδικα. Το IKEv2 είναι εξαιρετικό για κινητές συσκευές χάρη στη δυνατότητά του να επανασυνδέεται γρήγορα όταν αλλάζεις δίκτυο. [4]

### Q2: Τι είναι η δρομολόγηση διπλού VPN ή Multi-Hop;

Το Multi-Hop δρομολογεί την κίνησή σου μέσω δύο ή περισσότερων διακομιστών VPN διαδοχικά. Αυτό προσθέτει δεύτερο επίπεδο κρυπτογράφησης και βοηθά να μένει κρυφή η πραγματική σου διεύθυνση IP από τον δεύτερο κόμβο αν παραβιαστεί ένας διακομιστής.

### Q3: Τι είναι η διαρροή WebRTC και πώς την αποτρέπει ένα VPN;

Το WebRTC είναι ένα πρωτόκολλο προγράμματος περιήγησης που μπορεί να αποκαλύψει τις πραγματικές τοπικές και δημόσιες διευθύνσεις IP σου ακόμη και όταν το VPN είναι ενεργό. Τα premium VPN μπλοκάρουν ή παραποιούν τα αιτήματα WebRTC στις εφαρμογές για υπολογιστή και κινητό και στις επεκτάσεις προγράμματος περιήγησης.

### Q4: Τι είναι οι διακομιστές μόνο με RAM και γιατί έχουν σημασία;

Οι παραδοσιακοί διακομιστές γράφουν δεδομένα σε σκληρούς δίσκους, που μπορούν να κατασχεθούν ή να παραβιαστούν. Οι διακομιστές μόνο RAM (χωρίς δίσκο) λειτουργούν εξ ολοκλήρου σε προσωρινή μνήμη (RAM). Όταν ο διακομιστής επανεκκινείται ή σβήνει, τα δεδομένα στη μνήμη διαγράφονται.

### Q5: Πώς παρακάμπτει η παραπλάνηση (obfuscation) τους αποκλεισμούς VPN;

Η συσκότιση (ή «Stealth VPN») μεταμφιέζει την κίνηση VPN ώστε να μοιάζει με συνηθισμένη κίνηση HTTPS (θύρα 443). Αυτό μπορεί να βοηθήσει στην παράκαμψη της Βαθιάς Επιθεώρησης Πακέτων (DPI) που χρησιμοποιούν κυβερνήσεις ή δίκτυα σχολείων/γραφείων για να αποκλείουν τα VPN.

# Σημείο ελέγχου 10: Συχνές ερωτήσεις για τα VPN – προχωρημένο επίπεδο (Μέρος D)

Εξερεύνησε τεχνικές και δομικές πτυχές των εικονικών ιδιωτικών δικτύων και των ασφαλών πρωτοκόλλων τούνελ.

### Q6: Τι είναι το Split Tunneling και πότε πρέπει να το χρησιμοποιήσω;

Το Split Tunneling σου επιτρέπει να επιλέγεις ποιες εφαρμογές δρομολογούνται μέσω του κρυπτογραφημένου τούνελ VPN και ποιες συνδέονται απευθείας στο διαδίκτυο. Χρησιμοποίησέ το για να δρομολογείς ευαίσθητες τραπεζικές εφαρμογές μέσω του VPN, ενώ τα τοπικά παιχνίδια συνδέονται απευθείας, αποφεύγοντας την καθυστέρηση που προσθέτει το VPN.

### Q7: Πώς λειτουργεί το προωθητικό απόρρητο (Forward Secrecy / Perfect Forward Secrecy);

Το PFS διασφαλίζει ότι δημιουργείται ένα μοναδικό, προσωρινό κλειδί κρυπτογράφησης για κάθε συνεδρία. Ακόμη και αν ένα ιδιωτικό κλειδί παραβιαστεί στο μέλλον, δεν μπορεί να χρησιμοποιηθεί για την αποκρυπτογράφηση παλαιότερων ή μελλοντικών συνεδριών, επειδή χρησιμοποίησαν ανεξάρτητα κλειδιά.

### Q8: Τι είναι οι συμμαχίες 5/9/14 Eyes και γιατί να με ενδιαφέρουν;

Η δικαιοδοσία μπορεί να επηρεάσει τη νομική διαδικασία που μπορεί να αντιμετωπίσει ένας πάροχος, αλλά ο πρακτικός κίνδυνος για την ιδιωτικότητα εξαρτάται επίσης από τα δεδομένα που διατηρεί ο πάροχος, την τεχνική αρχιτεκτονική, την ιδιοκτησία, την έκδοση εκθέσεων διαφάνειας και το ιστορικό ελέγχων.

### Q9: Τι είναι η προστασία από διαρροές DNS;

Η προστασία από διαρροές DNS αναγκάζει τη συσκευή σου να στέλνει τα ερωτήματα αναζήτησης ιστοτόπων (ερωτήματα DNS) μέσω των ιδιωτικών, κρυπτογραφημένων διακομιστών DNS του VPN αντί για τους διακομιστές του παρόχου internet σου. Έτσι ο πάροχος δεν μπορεί να παρακολουθεί ποιους ιστοτόπους επισκέπτεσαι.

### Q10: Μπορεί ένα VPN να παρακάμψει τον περιορισμό ταχύτητας του πάροχου ίντερνετ;

Μερικές φορές. Ένα VPN μπορεί να βοηθήσει όταν ένας πάροχος διαδικτύου επιβραδύνει επιλεκτικά αναγνωρίσιμες δραστηριότητες, αλλά δεν θα ξεπεράσει τη συμφόρηση, τα όρια δεδομένων, τα όρια ταχύτητας σε επίπεδο λογαριασμού ή την κακή ποιότητα δικτύου.

# Τεχνικές αναφορές και πηγές

Παρατιθέμενες δημοσιεύσεις, κρυπτογραφικές προδιαγραφές και επίσημα πρότυπα εγγράφων που χρησιμοποιούνται σε αυτό το φύλλο εργασίας.

## ΑΚΑΔΗΜΑΪΚΕΣ ΚΑΙ ΒΙΟΜΗΧΑΝΙΚΕΣ ΑΝΑΦΟΡΕΣ

[1] NIST. (2020). SP 800-77 Rev. 1: Guide to IPsec VPNs.
https://csrc.nist.gov/pubs/sp/800/77/r1/final

[2] WireGuard. (n.d.). WireGuard: fast, modern, secure VPN tunnel.
https://www.wireguard.com/

[3] WireGuard. (n.d.). Protocol & Cryptography.
https://www.wireguard.com/protocol/

[4] Donenfeld, J. A. (2017). WireGuard: Next Generation Kernel Network Tunnel. NDSS Symposium.
https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/wireguard-next-generation-kernel-network-tunnel/

[5] OpenVPN. (n.d.). OpenVPN 2.6 Manual.
https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/

[6] IETF. (1999). RFC 2637: Point-to-Point Tunneling Protocol (PPTP).
https://datatracker.ietf.org/doc/html/rfc2637