Όνομα: _____ Ημερομηνία: _____ Βαθμολογία: _____

WireGuard εναντίον OpenVPN Φύλλο εργασίας

Σύγκριση των πρωτοκόλλων WireGuard και OpenVPN, των μεγεθών βάσης κώδικα, της ταχύτητας και των κρυπτογραφικών προτύπων

ΕΠΙΣΚΟΠΗΣΗ ΜΑΘΗΣΗΣ VPN

ΜΑΘΗΤΗΣ

ΙΔΙΟΤΗΤΑ ΦΟΙΤΗΤΗ

Διαδρομή Network Defender

ΑΣΦΑΛΕΣ

ΚΑΤΑΣΤΑΣΗ ΣΥΝΔΕΣΗΣ

Θωράκιση πακέτων δεδομένων

ΕΝΕΡΓΟ

ΠΡΟΣΤΑΣΙΑ ΔΙΑΡΡΟΩΝ

Προστασία από διαρροές DNS και IPv6

Καλώς ήρθες! Αυτό το φυλλάδιο δραστηριοτήτων σε καθοδηγεί στις βασικές αρχές των εικονικών ιδιωτικών δικτύων (VPN). Θα εξερευνήσεις πώς οι κρυπτογραφημένες σήραγγες ασφαλίζουν τα δεδομένα σου, πώς λειτουργούν τα πρωτόκολλα δικτύου και πώς να εντοπίζεις και να περιορίζεις τις διαρροές ιδιωτικότητας.

ΣΗΜΕΙΑ ΕΛΕΓΧΟΥ ΤΟΥ ΦΥΛΛΟΥ ΕΡΓΑΣΙΑΣ

- [ ] **Μέρη 1-4: Κατάκτησε τις έννοιες και τα πρωτόκολλα των VPN.**
- [ ] **Μέρη 5-7: Λύσε γρίφους σταυρολέξου και αναζήτησης λέξεων.**
- [ ] **Μέρη 8-9: Λύσε μελέτες περίπτωσης και πρόκληση κρυπτογραφημένου μηνύματος.**
- [ ] **Μέρος 10: Εξέτασε τις σελίδες συχνών ερωτήσεων βασικού και προχωρημένου επιπέδου.**
- [ ] **Μέρος 11: Εξερεύνησε 10 ενδιαφέροντα πραγματικά στοιχεία.**
- [ ] **Μπόνους: η πρόκληση Σκέψου γρήγορα.**

Άνοιξε τον Οδηγό του VPN.com για τα VPN

URL: https://www.vpn.com/el/vpn/

Η πορεία μάθησής σου: VPN

- Σύγκρινε την πολυπλοκότητα της βάσης κώδικα και την ταχύτητα ελέγχου των πρωτοκόλλων.
- Ανάλυσε τα οφέλη απόδοσης από την εκτέλεση μέσα στον χώρο του πυρήνα.
- Αντιπαράθεσε τους αλγορίθμους κρυπτογράφησης OpenSSL με τη σύγχρονη κρυπτογραφία του WireGuard.
- Δημιούργησε ζεύγη δημόσιου και ιδιωτικού κλειδιού για τις χειραψίες μεταξύ ομότιμων κόμβων.
- Δρομολογεί την κίνηση VPN μέσω θυρών τείχους προστασίας TCP και UDP.

ΟΔΗΓΙΕΣ ΦΥΛΛΟΥ ΕΡΓΑΣΙΑΣ ΣΥΓΚΡΙΣΗΣ ΠΡΩΤΟΚΟΛΛΩΝ

Απάντησε στις ερωτήσεις πολλαπλής επιλογής και σωστού/λάθους, συμπλήρωσε τα κενά των προτάσεων με την τράπεζα λέξεων, αντιστοίχισε ορισμούς και λύσε το σταυρόλεξο και τον γρίφο αναζήτησης λέξεων. Εφάρμοσε τις γνώσεις σου στον έλεγχο των σύγχρονων πρωτοκόλλων. Ολοκλήρωσε με τη δραστηριότητα μπόνους Σκέψου γρήγορα.

WIREGUARD ENANTI OPENVPN (ΕΙΣΑΓΩΓΗ)

Η επιλογή ενός πρωτοκόλλου VPN απαιτεί ισορροπία ανάμεσα στην ταχύτητα και τις επιλογές ρύθμισης. Το OpenVPN αποτελεί το πρότυπο εδώ και δεκαετίες, προσφέροντας ευελιξία ρύθμισης TCP/UDP. Το WireGuard είναι ένας σύγχρονος αντικαταστάτης που εκτελείται απευθείας στον χώρο του πυρήνα με μόλις 4.000 γραμμές κώδικα. Η κατανόηση των διαφορών των πρωτοκόλλων είναι το κλειδί για τη βελτιστοποίηση των ασφαλών δικτύων σου.

ΔΙΑΒΑΣΕ ΠΡΟΣΕΚΤΙΚΑ ΚΑΘΕ ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ ΚΑΙ ΕΠΙΛΕΞΕ Η ΓΡΑΨΕ ΤΗ ΣΩΣΤΗ ΑΠΑΝΤΗΣΗ.

Σημείο ελέγχου 1: Πρόκληση πολλαπλής επιλογής

1. **1. Ποιο είναι το κατά προσέγγιση μέγεθος του κώδικα του πρωτοκόλλου WireGuard;**
   - A. Περίπου 70.000 γραμμές
   - B. Πάνω από 100.000 γραμμές
   - C. Λιγότερες από 1.000 γραμμές
   - D. Περίπου 4.000 γραμμές

2. **2. Σε ποιον χώρο του λειτουργικού συστήματος εκτελείται το WireGuard;**
   - A. Χώρος χρήστη
   - B. Χώρος πυρήνα
   - C. Χώρος εφαρμογής
   - D. Εικονικός χώρος

3. **3. Σε ποια κρυπτογραφική βιβλιοθήκη βασίζεται κυρίως το OpenVPN;**
   - A. ChaCha20-Poly1305
   - B. Κρυπτογραφική βιβλιοθήκη OpenSSL
   - C. Πλαίσιο πρωτοκόλλου Noise
   - D. Κωδικοποίηση DES χωρίς κρυπτογράφηση

4. **4. Ποιο είναι ένα βασικό πλεονέκτημα απόδοσης του WireGuard έναντι του OpenVPN;**
   - A. Ταχύτερες χειραψίες σύνδεσης και χαμηλότερη καθυστέρηση
   - B. Παρακάμπτοντας την ανάγκη για δημόσιες διευθύνσεις IP
   - C. Ενσωματωμένη εγγενής υποστήριξη για παλαιού τύπου dial-up
   - D. Μηδενική επιβάρυνση μπαταρίας σε κινητές συσκευές

5. **5. Πώς πιστοποιεί το WireGuard τις συνδέσεις ομότιμων;**
   - A. Με την ανταλλαγή τυπικών κωδικών πρόσβασης χρηστών
   - B. Με την επαλήθευση των πιστοποιητικών καταχώρισης ονόματος τομέα
   - C. Με τη χρήση στατικών ζευγών δημόσιου και ιδιωτικού κλειδιού
   - D. Με έλεγχο των σειριακών αριθμών υλικού

Σημείο ελέγχου 2: Πρόκληση Σωστό ή Λάθος

6 Ερώτηση 6

6. Η συμπαγής βάση κώδικα του WireGuard την κάνει σημαντικά ευκολότερη στον έλεγχο.

Σωστό Λάθος

7 Ερώτηση 7

7. Το OpenVPN είναι γενικά ταχύτερο από το WireGuard επειδή εκτελείται στον χώρο πυρήνα.

Σωστό Λάθος

8 Ερώτηση 8

8. Το OpenVPN είναι άκρως ρυθμιζόμενο και υποστηρίζει τόσο UDP όσο και TCP.

Σωστό Λάθος

9 Ερώτηση 9

9. Το WireGuard χρησιμοποιεί σύγχρονη κρυπτογραφία όπως το ChaCha20 για γρήγορη κρυπτογράφηση πακέτων.

Σωστό Λάθος

10 Ερώτηση 10

10. Το WireGuard απαιτεί σύνθετες ρυθμίσεις αρχής πιστοποίησης για την ταυτοποίηση.

Σωστό Λάθος

Σημείο ελέγχου 3: Συμπλήρωση βασικών όρων

Διάβασε κάθε πρόταση παρακάτω και συμπλήρωσε το κενό με τον σωστό όρο από την Τράπεζα Λέξεων.

1. Το σύγχρονο πρωτόκολλο _____ λειτουργεί απευθείας μέσα στον πυρήνα του λειτουργικού.

2. Το παλαιότερο πρωτόκολλο _____ βασίζεται στη βιβλιοθήκη κρυπτογράφησης OpenSSL.

3. Η εκτέλεση κώδικα μέσα στον _____ του λειτουργικού μειώνει την επιβάρυνση εναλλαγής περιβάλλοντος.

4. Το OpenVPN εκτελείται στον χώρο του _____ , δρομολογώντας πακέτα μέσω εικονικών διεπαφών.

5. Το WireGuard χρησιμοποιεί δημόσια και ιδιωτικά _____ για να αναγνωρίζει τους ομότιμους κόμβους σύνδεσης.

6. Το μικρό μέγεθος της βάσης κώδικα ενισχύει την ασφάλεια του λογισμικού ως προς την _____ .

ΤΡΑΠΕΖΑ ΛΕΞΕΩΝ

ΕΛΕΓΞΙΜΟΤΗΤΑ ΖΕΥΓΗ ΚΛΕΙΔΙΩΝ ΠΥΡΗΝΑ ΧΡΗΣΤΗ OPENSSL OPENVPN TCP/UDP WIREGUARD

Γράψε τις απαντήσεις σου εδώ:

1. **2.**

3. **4.**

5. **6.**

Σημείο ελέγχου 4: Αντιστοίχιση εννοιών δικτύου

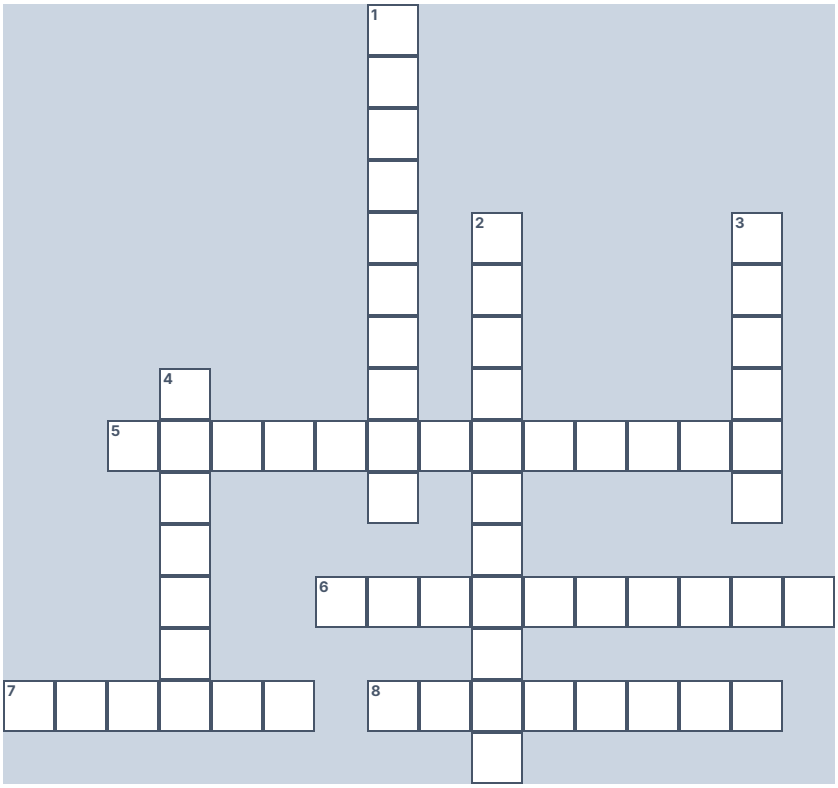
ΑΝΤΙΣΤΟΙΧΙΣΗ ΟΡΙΣΜΩΝ

Αντιστοίχισε κάθε όρο λεξιλογίου στα αριστερά με τον σωστό ορισμό του στα δεξιά, γράφοντας το αντίστοιχο γράμμα (A-H) στο πλαίσιο εισαγωγής.

☐	1. WireGuard	A	Χώρος εκτέλεσης όπου τρέχει το OpenVPN, δημιουργώντας επιβάρυνση εναλλαγής περιβάλλοντος.
☐	2. OpenVPN	B	Το μικρό μέγεθος της βάσης κώδικα του WireGuard, που την κάνει πολύ ευκολότερη στον έλεγχο.
☐	3. Χώρος πυρήνα	C	Κρυπτογραφική βιβλιοθήκη στην οποία βασίζεται το OpenVPN για τους αλγορίθμους κρυπτογράφησης.
☐	4. Χώρος χρήστη	D	Πρωτόκολλα μεταφοράς που υποστηρίζει το OpenVPN· το ίδιο το WireGuard λειτουργεί μόνο πάνω από UDP.
☐	5. 4.000 γραμμές	E	Περιοχή εκτέλεσης του λειτουργικού συστήματος όπου τρέχει το WireGuard για ταχύτητα.
☐	6. OpenSSL	F	Ασύμμετρα διακριτικά που χρησιμοποιεί το WireGuard για την επαλήθευση των συνδέσεων μεταξύ ομότιμων κόμβων.
☐	7. Ζεύγος κλειδιών	G	Σύγχρονο πρωτόκολλο VPN σχεδιασμένο για υψηλή ταχύτητα και απλό έλεγχο κώδικα.
☐	8. TCP/UDP	H	Ισχυρό παλαιό πρωτόκολλο που χρησιμοποιεί μεγάλη, σύνθετη βάση κώδικα ρυθμίσεων.

Σημείο ελέγχου 5: Σταυρόλεξο

Λύσε το σταυρόλεξο πληκτρολογώντας γράμματα στα ενεργά λευκά κουτιά. Οι αριθμοί αντιστοιχούν στις οδηγίες παρακάτω.



ΟΡΙΖΟΝΤΙΑ

5. Ασύμμετρα διακριτικά που χρησιμοποιεί το WireGuard για την επαλήθευση των ομότιμων συνδέσεων (13)

6. Σύγχρονο σύνολο κανόνων VPN σχεδιασμένο για υψηλή ταχύτητα και απλό έλεγχο κώδικα (10)

7. Η περιοχή εκτέλεσης όπου τρέχει το OpenVPN, δημιουργώντας επιβάρυνση εναλλαγής περιβάλλοντος (χώρος χρήστη) (6)

8. Πρωτόκολλα μεταφοράς που υποστηρίζει το OpenVPN (TCP/UDP)· το WireGuard τρέχει μόνο πάνω από UDP (8)

ΚΑΘΕΤΑ

1. Συλλογή κρυπτογραφικών αλγορίθμων στην οποία βασίζεται το OpenVPN (10)

2. Το μειονέκτημα ενός στιβαρού παλαιότερου VPN με μεγάλη βάση κώδικα και πολλές ρυθμίσεις (11)

3. Η περιοχή εκτέλεσης του λειτουργικού συστήματος όπου τρέχει το WireGuard για ταχύτητα (πυρήνας) (6)

4. Το συμπαγές μέγεθος της βάσης κώδικα του WireGuard, που την κάνει πολύ ευκολότερη στον έλεγχο (7)

Σημείο ελέγχου 5, εναλλακτικά: Προσβάσιμες ενδείξεις σταυρολέξου

Οι χρήστες αναγνώστη οθόνης και πληκτρολογίου μπορούν να πληκτρολογήσουν τις απαντήσεις του σταυρολέξου απευθείας στα πεδία κειμένου παρακάτω.

ΟΡΙΖΟΝΤΙΑ

5 οριζόντια: Ασύμμετρα διακριτικά που χρησιμοποιεί το WireGuard για την επαλήθευση των ομότιμων συνδέσεων (13 γράμματα):

6 οριζόντια: Σύγχρονο σύνολο κανόνων VPN σχεδιασμένο για υψηλή ταχύτητα και απλό έλεγχο κώδικα (10 γράμματα):

7 οριζόντια: Η περιοχή εκτέλεσης όπου τρέχει το OpenVPN, δημιουργώντας επιβάρυνση εναλλαγής περιβάλλοντος (χώρος χρήστη) (6 γράμματα):

8 οριζόντια: Πρωτόκολλα μεταφοράς που υποστηρίζει το OpenVPN (TCP/UDP)· το WireGuard τρέχει μόνο πάνω από UDP (8 γράμματα):

ΚΑΘΕΤΑ

1 κάθετα: Συλλογή κρυπτογραφικών αλγορίθμων στην οποία βασίζεται το OpenVPN (10 γράμματα):

2 κάθετα: Το μειονέκτημα ενός στιβαρού παλαιότερου VPN με μεγάλη βάση κώδικα και πολλές ρυθμίσεις (11 γράμματα):

3 κάθετα: Η περιοχή εκτέλεσης του λειτουργικού συστήματος όπου τρέχει το WireGuard για ταχύτητα (πυρήνας) (6 γράμματα):

4 κάθετα: Το συμπαγές μέγεθος της βάσης κώδικα του WireGuard, που την κάνει πολύ ευκολότερη στον έλεγχο (7 γράμματα):

Σημείο ελέγχου 6: Αναζήτηση κρυμμένων λέξεων

Βρες τους 8 βασικούς όρους λεξιλογίου που κρύβονται στο παρακάτω πλέγμα. Οι λέξεις μπορεί να είναι οριζόντιες, κάθετες ή διαγώνιες.

Γ Μ Α Ω Ψ Ζ Ψ Π Ξ Φ Υ Λ Υ Ο Β

Α Ν Ρ Φ Τ Μ Η Ρ Υ Γ Ψ Υ Κ Ρ Π

Τ Α Ο Χ Ω Ψ Μ Ω Ρ Π Χ Θ Ξ Υ Δ

Η Α Φ Γ Κ Π Φ Τ Χ Χ Λ Ι Ρ Θ Τ

Τ Θ Α Ζ Β Ε Θ Ο Κ Σ Ρ Η Φ Π Ω

Ο Ε Τ Θ Ε Ρ Γ Κ Α Λ Ν Ο Γ Ω Μ

Τ Κ Ε Φ Ρ Υ Α Ο Ρ Α Χ Κ Μ Μ Η

Ε Θ Μ Ν Θ Π Ζ Λ Η Τ Σ Η Ρ Χ Λ

Θ Σ Λ Ρ Χ Θ Β Λ Τ Ζ Ψ Ξ Ψ Χ Σ

Ν Η Τ Χ Α Ο Υ Ο Μ Ε Γ Ε Θ Ο Σ

Υ Ζ Ε Υ Γ Η Κ Λ Ε Ι Δ Ι Ω Ν Ν

Σ Ν Ω Ξ Θ Ο Σ Θ Ο Υ Τ Ξ Υ Τ Κ

Α Ε Β Ι Β Λ Ι Ο Θ Η Κ Η Ξ Μ Λ

Α Ν Υ Ζ Η Ο Π Χ Ψ Ι Κ Υ Ι Ω Φ

Ψ Ο Κ Θ Ω Ι Ι Ν Α Ε Θ Α Σ Α Ι

ΛΙΣΤΑ ΛΕΞΕΩΝ

ΠΡΩΤΟΚΟΛΛΟ ΣΥΝΘΕΤΟΤΗΤΑ ΠΥΡΗΝΑ ΧΡΗΣΤΗ ΜΕΓΕΘΟΣ ΒΙΒΛΙΟΘΗΚΗ ΖΕΥΓΗΚΛΕΙΔΙΩΝ ΜΕΤΑΦΟΡΑ

Σημείο ελέγχου 6, εναλλακτικά: Προσβάσιμη αντιστοίχιση λεξιλογίου

Αντιστοίχισε καθέναν από τους 8 όρους λεξιλογίου του Word Search με τον σωστό ορισμό του, γράφοντας το γράμμα (A-H) στο κενό.

ΟΡΟΙ ΛΕΞΙΛΟΓΙΟΥ

A. ΠΡΩΤΟΚΟΛΛΟ

B. ΣΥΝΘΕΤΟΤΗΤΑ

C. ΠΥΡΗΝΑ

D. ΧΡΗΣΤΗ

E. ΜΕΓΕΘΟΣ

F. ΒΙΒΛΙΟΘΗΚΗ

G. ΖΕΥΓΗΚΛΕΙΔΙΩΝ

H. ΜΕΤΑΦΟΡΑ

ΟΡΙΣΜΟΙ ΚΑΙ ΠΕΔΙΑ ΑΝΤΙΣΤΟΙΧΙΣΗΣ

1. Συλλογή κρυπτογραφικών αλγορίθμων στην οποία βασίζεται το OpenVPN.

2. Η περιοχή εκτέλεσης του λειτουργικού συστήματος όπου τρέχει το WireGuard για ταχύτητα (πυρήνας).

3. Το μειονέκτημα ενός στιβαρού παλαιότερου VPN με μεγάλη βάση κώδικα και πολλές ρυθμίσεις.

4. Ασύμμετρα διακριτικά που χρησιμοποιεί το WireGuard για την επαλήθευση των ομότιμων συνδέσεων.

5. Πρωτόκολλα μεταφοράς που υποστηρίζει το OpenVPN (TCP/UDP)· το WireGuard τρέχει μόνο πάνω από UDP.

6. Το συμπαγές μέγεθος της βάσης κώδικα του WireGuard, που την κάνει πολύ ευκολότερη στον έλεγχο.

7. Σύγχρονο σύνολο κανόνων VPN σχεδιασμένο για υψηλή ταχύτητα και απλό έλεγχο κώδικα.

8. Η περιοχή εκτέλεσης όπου τρέχει το OpenVPN, δημιουργώντας επιβάρυνση εναλλαγής περιβάλλοντος (χώρος χρήστη).

Σημείο ελέγχου 7: Πρόκληση ανακατεμένων λέξεων

Αποκωδικοποίησε τα γράμματα παρακάτω για να αποκαλύψεις βασικές έννοιες και όρους των VPN. Γράψε τις απαντήσεις σου στα πλαίσια εισαγωγής.

1. ΛΟΚΟΡΠΛΟΤΩ
2. ΑΠΡΝΗΥ
3. ΕΜΘΣΓΟΕ
4. ΚΩΙΥΕΗΝΛΙΔΖΕΓ
5. ΗΥΤΟΝΑΕΤΣΤΘ
6. ΤΣΧΗΗΡ
7. ΙΛΒΘΟΗΚΗΙΒ
8. ΑΕΦΑΜΡΟΤ

Δραστηριότητα μπόνους: Σκέψου γρήγορα

3 ΑΠΑΝΤΗΣΕΙΣ ΓΙΑ ΚΑΘΕ ΚΑΤΗΓΟΡΙΑ. ΚΕΡΔΙΖΕΙ ΟΠΟΙΟΣ ΣΥΜΠΛΗΡΩΣΕΙ ΠΡΩΤΟΣ ΤΗ ΛΙΣΤΑ.

1	Λόγοι για να επιλέξεις το WireGuard			
2	Υποσχέσεις που δίνει ένας καλός πάροχος VPN			
3	Λόγοι για να επιλέξεις το OpenVPN			
4	Λόγοι για να χρησιμοποιείς VPN όταν ταξιδεύεις			
5	Πράγματα που μπορεί να δει ο πάροχος internet σου			
6	Τρόποι να εντοπίσεις ένα ψεύτικο δίκτυο Wi-Fi			
7	Μύθοι για τα VPN			
8	Μέρη όπου θα χρησιμοποιούσες ένα VPN			
9	Γρήγορα πράγματα της καθημερινής ζωής			
10	Πράγματα από τα οποία ένα VPN δεν μπορεί να σε προστατεύσει			
11	Πράγματα που κάνουν έναν κώδικα ευκολότερο στον έλεγχο			
12	Πράγματα που ένα VPN μπορεί να κρύψει			
13	Διαφορές ανάμεσα στο WireGuard και στο OpenVPN			
14	Λέξεις που σχετίζονται με το απόρρητο			
15	Ονόματα κρυπτογράφησης που γνωρίζεις			

Σημείο ελέγχου 8: Μελέτες περίπτωσης VPN

Εφάρμοσε τις έννοιες που έμαθες για να λύσεις τα παρακάτω σενάρια πραγματικού κόσμου.

SARAH (ΦΟΙΤΗΤΡΙΑ ΣΤΟ ΚΑΦΕ)

👩‍💻 «Γεια! Είμαι στο Wi-Fi της καφετέριας και η εφαρμογή VPN μου με αφήνει να επιλέξω WireGuard ή OpenVPN. Οι βιντεοκλήσεις μου διακόπτονται συνέχεια όταν περπατάω ανάμεσα στο δίκτυο της καφετέριας και το hotspot του κινητού μου. Ποιο πρωτόκολλο να διαλέξω και γιατί θα χειριζόταν καλύτερα την εναλλαγή;»

ALEX (ΦΟΙΤΗΤΗΣ ΠΟΥ ΤΑΞΙΔΕΥΕΙ)

👩‍💻 «Είμαι στο εξωτερικό σε δίκτυο ξενοδοχείου που φαίνεται να αποκλείει το μεγαλύτερο μέρος της κίνησης VPN. Το WireGuard δεν συνδέεται καθόλου, αλλά πρέπει να έχω πρόσβαση στους πόρους του σχολείου μου στη χώρα μου. Τι πιθανόν αποκλείεται και πώς θα με βοηθούσε το OpenVPN να περάσω;»

Σημείο ελέγχου 9: Αποκρυπτογράφησε τον κώδικα

Για να ολοκληρώσεις την εκπαίδευσή σου στον έλεγχο πρωτοκόλλων, αποκρυπτογράφησε αυτό το κρυφό μήνυμα για την εκτέλεση σε χώρο πυρήνα.

ΚΛΕΙΔΙ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ ΓΡΑΜΜΑΤΟΣ ΣΕ ΑΡΙΘΜΟ

Α=1 Β=2 Γ=3 Δ=4 Ε=5 Ζ=6 Η=7 Θ=8

Ι=9 Κ=10 Λ=11 Μ=12 Ν=13 Ξ=14 Ο=15 Π=16

Ρ=17 Σ=18 Τ=19 Υ=20 Φ=21 Χ=22 Ψ=23 Ω=24

1	13	1	2	1	8	12	9	18	5		19	7		18	20	13	4	5	18	7
12	5		3	17	7	3	15	17	15	19	5	17	7							
18	7	17	1	3	3	1														

Αποκρυπτογραφημένο μήνυμα:

ΣΥΜΒΟΥΛΗ: ΚΑΘΕ ΑΡΙΘΜΟΣ ΕΚΠΡΟΣΩΠΕΙ ΤΗ ΘΕΣΗ ΤΟΥ ΓΡΑΜΜΑΤΟΣ ΣΤΟ ΑΛΦΑΒΗΤΟ (Π.Χ. 1 = Α, 2 = Β, 24 = Ω).

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 έχουν σημασία τα πρωτόκολλα;

Το πρωτόκολλο αποφασίζει πώς το VPN σου δημιουργεί τη σήραγγά του, ποια κρυπτογραφία προστατεύει τα δεδομένα σου και πόσο γρήγορα συνδέεται και επανασυνδέεται. Τα WireGuard και OpenVPN είναι τα δύο πρωτόκολλα ανοιχτού κώδικα που προσφέρουν οι περισσότερες εφαρμογές VPN, και κάνουν διαφορετικούς συμβιβασμούς ανάμεσα σε απλότητα, ταχύτητα και δυνατότητες ρύθμισης.

Q3: Είναι κάποιο από τα δύο πιο ιδιωτικό από το άλλο;

Κανένα από τα δύο πρωτόκολλα δεν σε κάνει ανώνυμο. Και τα δύο κρυπτογραφούν την κίνηση του τούνελ με ισχυρούς κρυπτογραφικούς αλγορίθμους· το απόρρητό σου εξαρτάται κυρίως από το τι καταγράφει ο πάροχος του VPN και πώς διαχειρίζεται τα κλειδιά, τους λογαριασμούς και τους διακομιστές.

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 και τα δύο ανοιχτού κώδικα;

Ναι. Τόσο το WireGuard όσο και η έκδοση κοινότητας του OpenVPN δημοσιεύουν τον πηγαίο κώδικά τους, ώστε ανεξάρτητοι ερευνητές να μπορούν να τον εξετάσουν. Ο μικρός κώδικας του WireGuard κάνει έναν πλήρη έλεγχο πολύ ταχύτερο.

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: Ποιο από τα δύο είναι ταχύτερο;

Το WireGuard είναι συνήθως ταχύτερο: τρέχει στον πυρήνα, χρησιμοποιεί ελαφριά κρυπτογράφηση ChaCha20-Poly1305 και ολοκληρώνει γρήγορα τις χειραψίες. Το OpenVPN έχει μεγαλύτερη επιβάρυνση, αλλά οι πραγματικές ταχύτητες εξαρτώνται και από το φορτίο και την απόσταση του διακομιστή.

Q7: Μπορούν και τα δύο να λειτουργήσουν μέσω TCP και UDP;

Όχι. Το OpenVPN μπορεί να τρέξει πάνω από UDP ή TCP και η λειτουργία TCP βοηθά σε δίκτυα που αποκλείουν το UDP. Το WireGuard στέλνει τα πακέτα του μόνο μέσω UDP, οπότε μπορεί να αποτύχει σε δίκτυα που επιτρέπουν μόνο TCP. [4]

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 WireGuard και OpenVPN στο κινητό μου;

Ναι. Το WireGuard είναι πολυπλατφορμικό, με εφαρμογές για Windows, macOS, Linux, iOS και Android, και υπάρχουν πελάτες OpenVPN για τα ίδια συστήματα. Οι περισσότερες εφαρμογές VPN σε αφήνουν να επιλέξεις όποιο θέλεις. [1]

Q10: Γιατί το WireGuard είναι τόσο μικρό;

Το WireGuard υποστηρίζει ένα σταθερό σύνολο σύγχρονων αλγορίθμων κρυπτογράφησης αντί για πολλές επιλογές. Η υλοποίησή του για Linux χρειάζεται λιγότερες από 4.000 γραμμές κώδικα, κάτι που το κάνει ευκολότερο στον έλεγχο από μεγαλύτερες βάσεις κώδικα VPN. [3]

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.

Q2: Ποιους κρυπτογραφικούς αλγορίθμους χρησιμοποιεί το WireGuard;

Το WireGuard χρησιμοποιεί ChaCha20 με Poly1305 για κρυπτογράφηση, Curve25519 για ανταλλαγή κλειδιών, BLAKE2s για κατακερματισμό και το πλαίσιο Noise για τη χειραψία του. Δεν υπάρχει διαπραγμάτευση αλγορίθμων, οπότε οι χρήστες δεν μπορούν να επιλέξουν μια αδύναμη επιλογή. [2]

Q3: Ποιους κρυπτογραφικούς αλγορίθμους και βιβλιοθήκες μπορεί να χρησιμοποιήσει το OpenVPN;

Το OpenVPN είναι στενά ενσωματωμένο με τη βιβλιοθήκη OpenSSL και χρησιμοποιεί TLS για την ανταλλαγή κλειδιών. Οι διαχειριστές μπορούν να επιλέξουν κρυπτογραφήσεις καναλιού δεδομένων όπως το AES-256-GCM, γεγονός που προσφέρει ευελιξία αλλά και περιθώριο για αδύναμες ρυθμίσεις. [4]

Q4: Πώς πιστοποιεί κάθε πρωτόκολλο τα ομότιμα μέρη (peers);

Οι ομότιμοι κόμβοι (peers) του WireGuard αναγνωρίζουν ο ένας τον άλλον με στατικά δημόσια κλειδιά, παρόμοια με την ανταλλαγή κλειδιών SSH, και κάθε κλειδί αντιστοιχίζεται σε επιτρεπόμενες IP σήραγγας. Το OpenVPN συνήθως βασίζεται σε μια αρχή πιστοποίησης με πιστοποιητικά X.509, συχνά σε συνδυασμό με όνομα χρήστη και κωδικό πρόσβασης.

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 συμβαίνει όταν αλλάζω από Wi-Fi σε δίκτυο κινητής;

Το WireGuard είναι χωρίς σύνδεση (connectionless): στέλνει πακέτα από τη νέα διεύθυνση και η σήραγγα συνεχίζεται μετά από μια γρήγορη χειραψία. Το OpenVPN διατηρεί κατάσταση συνεδρίας, οπότε μια αλλαγή δικτύου μπορεί να απαιτεί επανασύνδεση που διαρκεί λίγο περισσότερο.

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: Είναι το OpenVPN ακόμη καλή επιλογή αν το WireGuard είναι ταχύτερο;

Ναι. Το OpenVPN είναι ώριμο και ευρέως χρησιμοποιούμενο, λειτουργεί μέσω TCP όταν το UDP είναι αποκλεισμένο και υποστηρίζει εταιρικές ρυθμίσεις βάσει πιστοποιητικών. Πολλοί πάροχοι προσφέρουν και τα δύο πρωτόκολλα ώστε οι χρήστες να αλλάζουν αν το ένα αποκλειστεί ή είναι αργό.

Q9: Ποιες θύρες χρησιμοποιούν;

Η τυπική θύρα του OpenVPN είναι η 1194, αλλά μπορεί να μεταφερθεί σε οποιαδήποτε θύρα UDP ή TCP, συμπεριλαμβανομένης της 443. Το WireGuard ακούει σε μια θύρα UDP που ορίζεται στη διαμόρφωσή του· η 51820 είναι η θύρα που χρησιμοποιείται στα επίσημα παραδείγματά του.

Q10: Ποιο πρωτόκολλο ρυθμίζεται ευκολότερα με το χέρι;

Το WireGuard είναι συνήθως απλούστερο: δημιουργείς ένα ζεύγος κλειδιών, ανταλλάσσεις δημόσια κλειδιά και απαριθμείς τις επιτρεπόμενες IP. Το OpenVPN χρειάζεται πιστοποιητικά, μια CA και περισσότερες επιλογές, αν και τα προφίλ .ovpn τα συγκεντρώνουν σε ένα αρχείο.

Μέρος 11: 10 ενδιαφέροντα στοιχεία και πραγματικές διαπιστώσεις για τα VPN

Εξέτασε αυτά τα πολύτιμα, πραγματικά στοιχεία και πληροφορίες για την ιστορία, την αγορά και την τεχνολογία των VPN.

1. ΤΟ ΠΡΩΤΟ ΠΡΩΤΟΚΟΛΛΟ VPN

Το PPTP (Point-to-Point Tunneling Protocol) αναπτύχθηκε από ομάδα προμηθευτών που περιλάμβανε τη Microsoft και δημοσιεύθηκε ως RFC 2637 τον Ιούλιο του 1999 για την υποστήριξη VPN απομακρυσμένης πρόσβασης. [6]

2. ΔΥΟ ΜΕΤΑΦΟΡΕΣ

Το OpenVPN μπορεί να μεταφέρει το τούνελ του μέσω UDP ή TCP, και στη λειτουργία TLS τα κανάλια ελέγχου και δεδομένων μοιράζονται μία θύρα. [4]

3. Η ΕΠΑΝΑΣΤΑΣΗ ΤΟΥ WIREGUARD

Το WireGuard διαθέτει μια εξαιρετικά απλοποιημένη βάση κώδικα, σχεδιασμένη για αποδοτικότητα, που την κάνει ευκολότερη στον έλεγχο για ευπάθειες ασφαλείας από τα παραδοσιακά πρωτόκολλα. [3]

4. ΣΥΓΧΡΟΝΗ ΚΡΥΠΤΟΓΡΑΦΙΑ

Το WireGuard συνδυάζει ChaCha20, Poly1305, Curve25519, BLAKE2s, SipHash24 και HKDF μέσα στο πλαίσιο πρωτοκόλλου Noise, χωρίς επιλογές κρυπτογράφησης που οι χρήστες θα μπορούσαν να ρυθμίσουν λανθασμένα. [2]

5. OPENSSL ΜΕΣΑ ΣΤΟ OPENVPN

Το OpenVPN είναι στενά ενσωματωμένο με τη βιβλιοθήκη OpenSSL και αντλεί από αυτήν πολλές από τις κρυπτογραφικές δυνατότητές του, συμπεριλαμβανομένου του TLS που χρησιμοποιείται για την ανταλλαγή κλειδιών. [4]

6. ΑΝΑΛΥΣΗ ΒΑΘΟΥΣ ΠΑΚΕΤΩΝ

Η βαθιά επιθεώρηση πακέτων (DPI) εξετάζει το περιεχόμενο των πακέτων και τα μοτίβα κίνησης, όχι μόνο τις κεφαλίδες, και ορισμένα τείχη προστασίας τη χρησιμοποιούν για να εντοπίζουν και να αποκλείουν συνηθισμένα πρωτόκολλα VPN.

7. ΚΛΕΙΔΙΑ ΤΥΠΟΥ SSH

Οι συνδέσεις WireGuard ρυθμίζονται με ανταλλαγή απλών δημόσιων κλειδιών, παρόμοια με την ανταλλαγή κλειδιών SSH, χωρίς να απαιτείται αρχή πιστοποίησης. [1]

8. ΠΟΛΛΑΠΛΕΣ ΠΛΑΤΦΟΡΜΕΣ

Το WireGuard κυκλοφόρησε αρχικά για τον πυρήνα Linux και πλέον είναι διαθέσιμο για Windows, macOS, BSD, iOS και Android, οπότε το ίδιο πρωτόκολλο λειτουργεί στις περισσότερες συσκευές. [1]

9. ΠΡΟΩΘΗΤΙΚΗ ΑΠΟΡΡΗΤΟΤΗΤΑ

Το WireGuard επαναλαμβάνει τη χειραψία Noise_IK κάθε λίγα λεπτά για να εναλλάσσει τα συμμετρικά κλειδιά συνεδρίας, παρέχοντας τέλεια προωθητική μυστικότητα (perfect forward secrecy) ακόμη και αν διαρρεύσει αργότερα ένα μακροπρόθεσμο κλειδί. [2]

10. ΔΙΕΠΑΦΕΣ TUN/TAP

Το OpenVPN έχει σχεδιαστεί να λειτουργεί με τη virtual διεπαφή δικτύου TUN/TAP, που είναι διαθέσιμη στις περισσότερες πλατφόρμες και μεταφέρει τα πακέτα του τούνελ. [4]

Τεχνικές αναφορές και πηγές

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

ΑΚΑΔΗΜΑΪΚΕΣ ΚΑΙ ΒΙΟΜΗΧΑΝΙΚΕΣ ΑΝΑΦΟΡΕΣ

[1] WireGuard. (n.d.). WireGuard: fast, modern, secure VPN tunnel.

https://www.wireguard.com/

[2] WireGuard. (n.d.). Protocol & Cryptography.

https://www.wireguard.com/protocol/

[3] 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/

[4] OpenVPN. (n.d.). OpenVPN 2.6 Manual.

https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/

[5] WireGuard. (n.d.). Quick Start.

https://www.wireguard.com/quickstart/

[6] IETF. (1999). RFC 2637: Point-to-Point Tunneling Protocol (PPTP).

https://datatracker.ietf.org/doc/html/rfc2637

Λύσεις: Σύγκριση των πρωτοκόλλων WireGuard και OpenVPN, του μεγέθους του κώδικα, της ταχύτητας και των κρυπτογραφικών προτύπων

1 **Μέγεθος κώδικα WireGuard** ΠΡΩΤΟΚΟΛΛΑ — **Σωστή απάντηση: D**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Το WireGuard είναι εξαιρετικά συμπαγές, με περίπου 4.000 γραμμές κώδικα. Αυτό διατηρεί μικρή την επιφάνεια επίθεσης και διευκολύνει τον έλεγχο. Παραπομπή: WireGuard Project.

2 **Ταχύτητα χώρου πυρήνα** ΚΑΘΥΣΤΕΡΗΣΗ — **Σωστή απάντηση: B**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Εκτελούμενο απευθείας στον χώρο του πυρήνα, το WireGuard αποφεύγει την επιβάρυνση της εναλλαγής περιβάλλοντος, επιτρέποντας υψηλή απόδοση (throughput). Παραπομπή: WireGuard Project.

3 **Ερώτηση 3** — **Σωστή απάντηση: B**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Το OpenVPN είναι στενά ενσωματωμένο με το OpenSSL, που παρέχει αλγόριθμους όπως το AES-GCM και το κάνει πολύ παραμετροποιήσιμο αλλά πιο σύνθετο.

4 **Απόδοση πρωτοκόλλου** ΕΛΕΓΧΟΙ ΔΡΟΜΟΛΟΓΗΣΗΣ — **Σωστή απάντηση: A**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Το WireGuard πραγματοποιεί χειραψίες σε χιλιοστά του δευτερολέπτου και ανταποκρίνεται άμεσα στην περιαγωγή δικτύου (π.χ. μετάβαση από Wi-Fi σε δίκτυο κινητής). Παραπομπή: Microsoft Native Gateway, Apple Support. [3]

5 **Ασύμμετρη κρυπτογραφία** ΙΔΙΩΤΙΚΟΤΗΤΑ — **Σωστή απάντηση: C**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Το WireGuard χρησιμοποιεί Cryptokey Routing, που συσχετίζει δημόσια κλειδιά με επιτρεπόμενες διευθύνσεις IP σήραγγας, παρόμοια με τις ρυθμίσεις SSH. Παραπομπή: WireGuard Project.

Λύσεις: Σημείο ελέγχου 2 – Σωστό ή Λάθος

6 Ερώτηση 6

Σωστή απάντηση: Σωστό

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Η υλοποίηση του WireGuard για Linux έχει λιγότερες από 4.000 γραμμές, οπότε οι ομάδες ασφάλειας μπορούν να την ελέγξουν πολύ ταχύτερα από πολύ μεγαλύτερες βάσεις κώδικα VPN, όπως το OpenVPN.

7 Καθυστέρηση χώρου χρήστη ΤΑΧΥΤΗΤΕΣ

Σωστή απάντηση: Λάθος

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Το OpenVPN εκτελείται στον χώρο χρήστη, μεταφέροντας πακέτα πέρα δώθε από τη virtual διεπαφή του πυρήνα, κάτι που προσθέτει επιβάρυνση αλλαγής περιβάλλοντος (εκτός αν χρησιμοποιείται εκφόρτωση στον πυρήνα, όπως το OpenVPN DCO). Παραπομπή: DD-WRT custom firmware.

8 Διαμόρφωση OpenVPN ΚΙΝΔΥΝΟΣ ΥΠΟΚΛΟΠΗΣ

Σωστή απάντηση: Σωστό

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Το OpenVPN υποστηρίζει λειτουργία μέσω TCP (για αξιοπιστία/παράκαμψη τειχών προστασίας) ή UDP (για ταχύτητα), γεγονός που το καθιστά συμβατό με σύνθετα εταιρικά τείχη προστασίας. Παραπομπή: IETF Cryptographic Protocols.

9 Σύγχρονη κρυπτογραφία ΤΕΙΧΗ ΠΡΟΣΤΑΣΙΑΣ

Σωστή απάντηση: Σωστό

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Το WireGuard απορρίπτει τους παλαιούς αλγορίθμους υπέρ σύγχρονων, ασφαλών πρωτογενών στοιχείων όπως τα ChaCha20 και Poly1305, που τρέχουν γρήγορα σε επεξεργαστές κινητών. Παραπομπή: WireGuard Project.

10 Απλοποίηση ζεύγους κλειδιών ΧΩΡΙΣ ΚΑΤΑΓΡΑΦΗ

Σωστή απάντηση: Λάθος

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Το WireGuard δεν χρησιμοποιεί πιστοποιητικά ή σύνθετες ιεραρχίες CA· βασίζεται σε απλά ζεύγη δημόσιου/ιδιωτικού κλειδιού που ανταλλάσσονται μεταξύ των ομότιμων κόμβων (peers). Παραπομπή: WireGuard Project.

Λύσεις λεξιλογίου και κριτήρια βαθμολόγησης

Κριτήρια βαθμολόγησης για τον εκπαιδευτικό: Δώσε 1 μονάδα για κάθε σωστή αντιστοίχιση (σύνολο 8 μονάδες) και για κάθε όρο περιεχομένου (σύνολο 6 μονάδες).

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 4: ΛΥΣΕΙΣ – ΑΝΤΙΣΤΟΙΧΙΣΗ ΕΝΝΟΙΩΝ

G 1. WireGuard	H 2. OpenVPN	E 3. Χώρος πυρήνα	A 4. Χώρος χρήστη
B 5. 4.000 γραμμές	C 6. OpenSSL	F 7. Ζεύγος κλειδιών	D 8. TCP/UDP

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 3: ΛΥΣΕΙΣ – ΒΑΣΙΚΟΙ ΟΡΟΙ

1 WIREGUARD	2 OPENVPN	3 ΠΥΡΗΝΑ	4 ΧΡΗΣΤΗ
5 ΖΕΥΓΗ ΚΛΕΙΔΙΩΝ	6 ΕΛΕΓΞΙΜΟΤΗΤΑ		

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 6, ΕΝΑΛΛΑΚΤΙΚΑ: ΛΥΣΕΙΣ – ΑΝΤΙΣΤΟΙΧΙΣΗ ΛΕΞΕΩΝ

1 F – ΒΙΒΛΙΟΘΗΚΗ	2 C – ΠΥΡΗΝΑ	3 B – ΣΥΝΘΕΤΟΤΗΤΑ	4 G – ΖΕΥΓΗΚΛΕΙΔΙΩΝ
5 H – ΜΕΤΑΦΟΡΑ	6 E – ΜΕΓΕΘΟΣ	7 A – ΠΡΩΤΟΚΟΛΛΟ	8 D – ΧΡΗΣΤΗ

ΣΗΜΕΙΩΣΕΙΣ ΣΥΖΗΤΗΣΗΣ ΓΙΑ ΕΚΠΑΙΔΕΥΤΙΚΟΥΣ

Βασικοί όροι:
Έλεγξε αν οι μαθητές μπορούν να εξηγήσουν με δικά τους λόγια τους όρους WireGuard, OpenVPN και Χώρος πυρήνα και να δώσουν ένα παράδειγμα για τον καθένα.

Μελέτες περίπτωσης:
Ζήτησε από τους μαθητές να στηρίζουν τις προτάσεις τους σε στοιχεία του φύλλου εργασίας και όχι σε υποθέσεις.

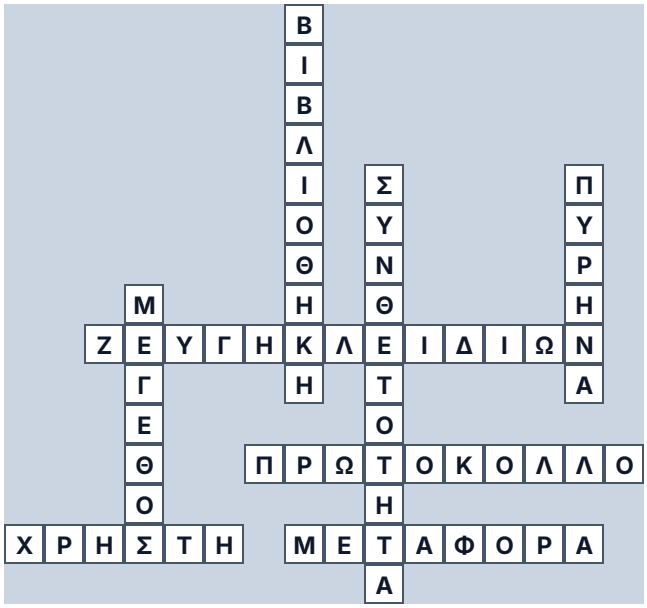
Αξιολόγηση πηγών:
Ζήτησε από τους μαθητές να επαληθεύσουν τουλάχιστον έναν ισχυρισμό στις πηγές του φύλλου και συζητήστε γιατί οι αριθμοί, οι τιμές και οι κανόνες μπορεί να αλλάζουν με τον χρόνο.

Λύσεις γρίφων και σημειώσεις για τον εκπαιδευτικό

ΛΥΣΗ ΓΡΙΦΟΥ ΛΕΞΕΩΝ

Γ	Μ	**Α**	Ω	Ψ	Ζ	Ψ	**Π**	Ξ	Φ	Υ	Λ	Υ	Ο	Β
Α	Ν	**Ρ**	Φ	Τ	Μ	Η	**Ρ**	Υ	Γ	Ψ	Υ	Κ	Ρ	**Π**
Τ	Α	**Ο**	Χ	Ω	Ψ	Μ	**Ω**	Ρ	Π	Χ	Θ	Ξ	**Υ**	Δ
Η	Α	**Φ**	Γ	Κ	Π	Φ	**Τ**	Χ	Χ	Λ	Ι	**Ρ**	Θ	Τ
Τ	Θ	**Α**	Ζ	Β	Ε	Θ	**Ο**	Κ	Σ	Ρ	**Η**	Φ	Π	Ω
Ο	Ε	**Τ**	Θ	Ε	Ρ	Γ	**Κ**	Α	Λ	**Ν**	Ο	Γ	Ω	Μ
Τ	Κ	**Ε**	Φ	Ρ	Υ	Α	**Ο**	Ρ	**Α**	Χ	Κ	Μ	Μ	Η
Ε	Θ	**Μ**	Ν	Θ	Π	Ζ	**Λ**	**Η**	**Τ**	**Σ**	**Η**	**Ρ**	**Χ**	Λ
Θ	Σ	Λ	Ρ	Χ	Θ	Β	**Λ**	Τ	Ζ	Ψ	Ξ	Ψ	Χ	Σ
Ν	Η	Τ	Χ	Α	Ο	Υ	**Ο**	**Μ**	**Ε**	**Γ**	**Ε**	**Θ**	**Ο**	**Σ**
Υ	**Ζ**	**Ε**	**Υ**	**Γ**	**Η**	**Κ**	**Λ**	**Ε**	**Ι**	**Δ**	**Ι**	**Ω**	**Ν**	Ν
Σ	Ν	Ω	Ξ	Θ	Ο	Σ	Θ	Ο	Υ	Τ	Ξ	Υ	Τ	Κ
Α	Ε	**Β**	**Ι**	**Β**	**Λ**	**Ι**	**Ο**	**Θ**	**Η**	**Κ**	**Η**	Ξ	Μ	Λ
Α	Ν	Υ	Ζ	Η	Ο	Π	Χ	Ψ	Ι	Κ	Υ	Ι	Ω	Φ
Ψ	Ο	Κ	Θ	Ω	Ι	Ι	Ν	Α	Ε	Θ	Α	Σ	Α	Ι

ΛΥΣΗ ΣΤΑΥΡΟΛΕΞΟΥ



ΟΔΗΓΟΣ ΕΚΠΑΙΔΕΥΤΙΚΟΥ ΓΙΑ ΤΙΣ ΛΥΣΕΙΣ ΤΟΥ ΣΤΑΥΡΟΛΕΞΟΥ

ΟΡΙΖΟΝΤΙΑ

5 οριζόντια: ΖΕΥΓΗΚΛΕΙΔΙΩΝ Ασύμμετρα διακριτικά που χρησιμοποιεί το WireGuard για την επαλήθευση των ομότιμων συνδέσεων (13 γράμματα)

6 οριζόντια: ΠΡΩΤΟΚΟΛΛΟ Σύγχρονο σύνολο κανόνων VPN σχεδιασμένο για υψηλή ταχύτητα και απλό έλεγχο κώδικα (10 γράμματα)

7 οριζόντια: ΧΡΗΣΤΗ Η περιοχή εκτέλεσης όπου τρέχει το OpenVPN, δημιουργώντας επιβάρυνση εναλλαγής περιβάλλοντος (χώρος χρήστη) (6 γράμματα)

8 οριζόντια: ΜΕΤΑΦΟΡΑ Πρωτόκολλα μεταφοράς που υποστηρίζει το OpenVPN (TCP/UDP)· το WireGuard τρέχει μόνο πάνω από UDP (8 γράμματα)

ΚΑΘΕΤΑ

1 κάθετα: ΒΙΒΛΙΟΘΗΚΗ Συλλογή κρυπτογραφικών αλγορίθμων στην οποία βασίζεται το OpenVPN (10 γράμματα)

2 κάθετα: ΣΥΝΘΕΤΟΤΗΤΑ Το μειονέκτημα ενός στιβαρού παλαιότερου VPN με μεγάλη βάση κώδικα και πολλές ρυθμίσεις (11 γράμματα)

3 κάθετα: ΠΥΡΗΝΑ Η περιοχή εκτέλεσης του λειτουργικού συστήματος όπου τρέχει το WireGuard για ταχύτητα (πυρήνας) (6 γράμματα)

4 κάθετα: ΜΕΓΕΘΟΣ Το συμπαγές μέγεθος της βάσης κώδικα του WireGuard, που την κάνει πολύ ευκολότερη στον έλεγχο (7 γράμματα)

Λύσεις: ανακατεμένες λέξεις και λύση κώδικα

Κλειδί βαθμολόγησης για τη δραστηριότητα αποκωδικοποίησης λέξεων λεξιλογίου και την πρόκληση Secret Cipher.

ΛΥΣΕΙΣ ΑΝΑΜΕΙΞΗΣ ΛΕΞΕΩΝ

1. ΛΟΚΟΡΠΛΟΤΩ — **ΠΡΩΤΟΚΟΛΛΟ**
2. ΑΠΡΝΗΥ — **ΠΥΡΗΝΑ**
3. ΕΜΘΣΓΟΕ — **ΜΕΓΕΘΟΣ**
4. ΚΩΙΥΕΗΝΛΙΔΖΕΓ — **ΖΕΥΓΗΚΛΕΙΔΙΩΝ**
5. ΗΥΤΟΝΑΕΤΣΤΘ — **ΣΥΝΘΕΤΟΤΗΤΑ**
6. ΤΣΧΗΗΡ — **ΧΡΗΣΤΗ**
7. ΙΛΒΘΟΗΚΗΙΒ — **ΒΙΒΛΙΟΘΗΚΗ**
8. ΑΕΦΑΜΡΟΤ — **ΜΕΤΑΦΟΡΑ**

ΚΛΕΙΔΙ ΠΡΟΚΛΗΣΗΣ ΜΥΣΤΙΚΟΥ ΚΩΔΙΚΑ

"ΑΝΑΒΑΘΜΙΣΕ ΤΗ ΣΥΝΔΕΣΗ ΜΕ ΓΡΗΓΟΡΟΤΕΡΗ ΣΗΡΑΓΓΑ"

Λύσεις των μελετών περίπτωσης

A Σενάριο Α: Επιλογή πρωτοκόλλου

ΥΠΟΚΛΟΠΗ ΚΑΙ ΚΡΥΠΤΟΓΡΑΦΗΣΗ

Το δίλημμα της Sarah

ΟΔΗΓΙΕΣ ΒΑΘΜΟΛΟΓΗΣΗΣ

Οι απαντήσεις των μαθητών πρέπει να καλύπτουν τα εξής σημεία:

- Σύσταση: WireGuard. Ο ελαφρύς σχεδιασμός του χωρίς σύνδεση (connectionless) επιτρέπει στη σήραγγα να ανακάμπτει γρήγορα όταν αλλάζει το δίκτυό της, ενώ το ChaCha20-Poly1305 διατηρεί γρήγορη την κρυπτογράφηση.
- Ασφάλεια: Και τα δύο πρωτόκολλα κρυπτογραφούν την κίνησή της στο Wi-Fi του καφέ, επομένως όποιο κι αν επιλέξει προστατεύει τις συνδέσεις της όταν είναι σωστά ρυθμισμένο· η επιλογή επηρεάζει κυρίως την ταχύτητα και τη σταθερότητα.

B Σενάριο Β: Παράκαμψη των αποκλεισμών VPN

ΓΕΩΓΡΑΦΙΚΟΣ ΑΠΟΚΛΕΙΣΜΟΣ ΚΑΙ IP

Το δίλημμα του Alex

ΟΔΗΓΙΕΣ ΒΑΘΜΟΛΟΓΗΣΗΣ

Οι απαντήσεις των μαθητών πρέπει να καλύπτουν τα εξής σημεία:

- Γιατί μπλοκαρίστηκε: Το WireGuard χρησιμοποιεί μόνο UDP, και το τείχος προστασίας του ξενοδοχείου πιθανότατα μπλοκάρει το UDP ή αναγνωρίζει τα πακέτα WireGuard μέσω φιλτραρίσματος ή Βαθιάς Επιθεώρησης Πακέτων (DPI).
- Πώς βοηθά το OpenVPN: Μπορεί να λειτουργήσει μέσω TCP, συμπεριλαμβανομένης της θύρας 443 που χρησιμοποιεί το HTTPS, την οποία τα τείχη προστασίας των ξενοδοχείων σπάνια αποκλείουν εντελώς επειδή η περιήγηση στο web εξαρτάται από αυτήν.