שם: _____ תאריך: _____ ציון: _____

האבטחה של Mullvad

ניתוח ארכיטקטורת האבטחה של Mullvad VPN, כולל שרתי RAM בלבד ללא דיסקים, מדיניות אפס יומנים שנבדקה בביקורת, יצירת מפתחות מקומית, הצפנת WireGuard והגדרות מנהרה עמידות בפני מחשוב קוונטי.

סקירת למידה: האבטחה של Mullvad

לומד

מעמד סטודנט

מסלול מגן הרשת

מאובטח

מצב חיבור

הגנה על מנות נתונים

פעיל

הגנה מפני דליפות

הגנה מפני דליפות DNS ו-IPv6

ברוכים הבאים! חוברת הפעילויות הזו תדריך אתכם דרך ארכיטקטורת האבטחה של Mullvad. תחקרו שרתי RAM בלבד ללא דיסק, מדיניות אפס יומנים מבוקרת, יצירת מפתחות מקומית ומנהרות עמידות לקוונטים.

נקודות הביקורת בדף העבודה

- ☐ **חלק 1-4: שלטו בהגדרות VPN ואבטחת רשת.**
- ☐ **חלק 5-7: פתרו תשבצים ופאזלי חיפוש מילים.**
- ☐ **חלק 8-9: פתרו מקרי בוחן ואתגר צופן.**
- ☐ **חלק 10: סקרו את דפי השאלות הנפוצות הבסיסיים והמתקדמים.**
- ☐ **חלק 11: חקרו 10 עובדות מעניינות מהעולם האמיתי.**
- ☐ **בונוס: אתגר חשבו מהר**

פתחו את מדריך ה-VPN הטובים ביותר של VPN.com

URL: https://www.vpn.com/vpn/mullvad/security/

מפת הלמידה שלכם: אבטחת Mullvad

- נתחו את הארכיטקטורה הטכנית וכללי ההגדרה של האבטחה של Mullvad.
- הגדירו את הגדרות הלקוח כדי למנוע דליפות תעבורה של IP, DNS ו-WebRTC.
- השוו תמחור מותאם אישית, תקופות ניסיון ותכונות ביצועים למודלים רגילים.

הוראות למדריך האבטחה של Mullvad

ענו על שאלות אמריקאיות ועל שאלות נכון/לא נכון, השלימו את המשפטים החסרים בעזרת בנק המילים, התאימו הגדרות ופתרו את התשבץ ואת תפזורת המילים. יישמו את הידע שלכם בנושא בקרות שרת של Mullvad המתמקדות בפרטיות. ולסיום, פעילות הבונוס "חשבו מהר".

הערכת תשתית שמעדיפה אלמוניות ודרגות RAM (מבוא)

Mullvad אינה משתמשת בחשבונות רגילים עם סיסמאות אלא נשענת על קודים אקראיים בני 16 ספרות. התשתית שלה בנויה מצמתי RAM בלבד ללא דיסק, מפתחות WireGuard שנוצרים מקומית ומדיניות אפס שימור שעברה ביקורת.

קראו כל נקודת ביקורת בעיון ובחרו או כתבו את התגובה הנכונה.

נקודת ביקורת 1: אתגר שאלות אמריקאיות

1 1. איזה פרוטוקול מנהור הוא ברירת המחדל באפליקציה של Mullvad?

- A) OpenVPN
- B) WireGuard
- C) IKEv2
- D) PPTP

2 2. מה Mullvad דורשת כדי ליצור חשבון חדש?

- A) שום דבר
- B) כתובת אימייל
- C) מספר טלפון
- D) מסמך זהות

3 3. איזו מנהרה קריפטוגרפית מגינה מפני מחשבים קוונטיים?

- A) AES-256-GCM
- B) Quantum WireGuard
- C) RSA-4096
- D) SOCKS5 Proxy

4 4. איזה מנגנון אבטחה חוסם סכנות של דליפות WebRTC?

- A) תוסף דפדפן
- B) Network Kill Switch
- C) ניתוב WebRTC דרך ממשק ה-VPN
- D) Split Tunneling

5 5. איזו תכונת multihop מנתבת תעבורה דרך כמה צמתים?

- A) NAT כפול
- B) WireGuard Multihop
- C) פרוטוקול Chameleon
- D) Bypasser

נקודת ביקורת 2: אתגר נכון או לא נכון

שאלה 6

6. Mullvad דורשת כתובת אימייל בעת הפקת חשבון.

נכון לא נכון

שאלה 7

7. אפשר להגדיר פרוקסי SOCKS5 בתוך מנהרות Mullvad.

נכון לא נכון

שאלה 8

8. Mullvad היא הבעלים של כל חומרת השרתים שלה ומפעילה אותה.

נכון לא נכון

שאלה 9

9. מתג הקטיעה של הרשת פעיל תמיד כברירת מחדל.

נכון לא נכון

שאלה 10

10. תשלומים במזומן שנשלחו בדואר אינם ניתנים להחזר כלל.

נכון לא נכון

נקודת ביקורת 3: השלמת מונחי מפתח

קראו כל משפט שלהלן והשלימו את החסר במונח הנכון מבנק המילים.

1. Mullvad נשענת על _____ כפרוטוקול המנהור המהיר והמאובטח העיקרי שלה.
2. ניתוב נתונים דרך שני מיקומי שרת נקרא תצורת _____ .
3. כדי למנוע יומני נתונים בדיסק, Mullvad פורסת צמתים ייעודיים מסוג _____ .
4. תעבורת המערכת נחסמת כשמנהרה נכשלת באמצעות מנגנון ההגנה המובנה: _____ .
5. הצהרות ביקורת מאשרות ש-Mullvad מקיימת ארכיטקטורת _____ קפדנית ומאומתת.
6. ניתן לבודד ניתוב פנימי של יישומים באמצעות הגדרת _____ SOCKS5 מותאמת.
7. אלגוריתמי הצפנה פוסט-קוונטיים מאבטחים נתונים בתוך מנהרה בעלת הגנה _____ .
8. שרתי שמות פרטיים נפרסים ברחבי העולם כדי לסייע בחסימת סכנות של _____ DNS.

בנק מילים

אפס יומנים | דליפות | ווירגארד | זיכרון בלבד קוונטית | מתג הפסקה | ניתוב כפול | פרוקסי

כתבו את תשובותיכם כאן:

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____
8. _____

נקודת ביקורת 4: התאמת מושגים ב-VPN וברשתות

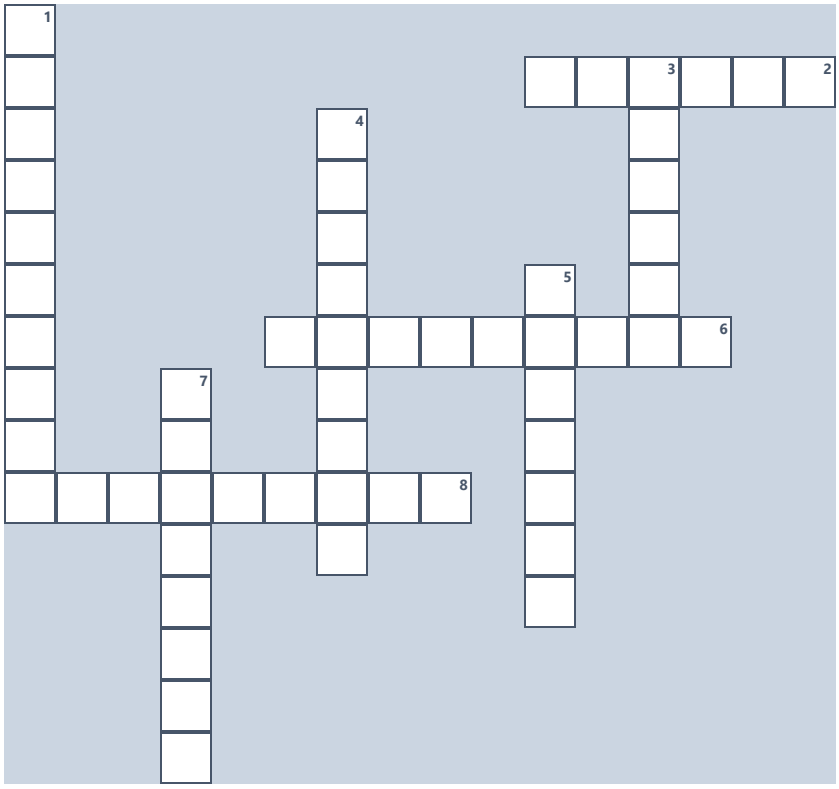
התאמת הגדרות

התאימו כל מונח אוצר מילים בצד ימין להגדרה הנכונה שלו בצד שמאל על ידי כתיבת האות המתאימה (A-H) בתיבת הקלט הניתנת למילוי.

1. ווירגארד	A	תכונת בטיחות שמנתקת תעבורה כשה-VPN נופל.
2. ניתוב כפול	B	פרוטוקול מנהור מאובטח קל משקל וביצועים גבוהים.
3. RAM בלבד	C	פרוטוקול פרוקסי פנימי המשמש לבידוד אפליקציות לקוח.
4. מתג הפסקה	D	ניתוב תעבורה דרך צומת שרת כניסה וצומת שרת יציאה.
5. אפס יומנים	E	מנגנוני הצפנה שנועדו לעמוד בפני התקפות קוונטיות.
6. פרוקסי	F	חשיפת יעדי שאילתות DNS מחוץ למנהרת ה-VPN.
7. קוונטית	G	חומרת שרת עם זיכרון נדיף שאינה שומרת נתונים לאחר אתחול.
8. דליפות	H	תקן אפס שמירת נתונים המאומת בביקורות עצמאיות.

נקודת ביקורת 5: תשבץ

פתרו את התשבץ על ידי הקלדת אותיות בתיבות הלבנות הפעילות. המספרים מתאימים לרמזים שלהלן.



מאוזן

2. חשיפת יעדי שאילתות DNS מחוץ למנהרת ה-VPN (6)

6. ניתוב תעבורה דרך צומת שרת כניסה וצומת שרת יציאה (9)

8. פרוטוקול מנהור מאובטח קל משקל ובעל ביצועים גבוהים (9)

מאונך

1. חומרת שרת עם זיכרון נדיף שאינה שומרת נתונים לאחר אתחול (10)

3. פרוטוקול ביניים פנימי המשמש לבידוד יישומי לקוח (6)

4. תקן אי-שמירת נתונים שאומת בביקורות עצמאיות (9)

5. מנגנוני הצפנה שנועדו לעמוד בפני התקפות quantum (7)

7. תכונת בטיחות שחותכת את התעבורה כשה-VPN נופל (8)

נקודת ביקורת 5 – פעילות חלופית: רמזים נגישים לתשבץ

משתמשי קורא מסך ומקלדת יכולים להקליד את תשובות התשבץ ישירות בשדות הטקסט שלהלן.

מאוזן

2 מאוזן: חשיפת יעדי שאילתות DNS מחוץ למנהרת ה-VPN (6 אותיות):

6 מאוזן: ניתוב תעבורה דרך צומת שרת כניסה וצומת שרת יציאה (9 אותיות):

8 מאוזן: פרוטוקול מנהור מאובטח קל משקל ובעל ביצועים גבוהים (9 אותיות):

מאונך

1 מאונך: חומרת שרת עם זיכרון נדיף שאינה שומרת נתונים לאחר אתחול (10 אותיות):

3 מאונך: פרוטוקול ביניים פנימי המשמש לבידוד יישומי לקוח (6 אותיות):

4 מאונך: תקן אי-שמירת נתונים שאומת בביקורות עצמאיות (9 אותיות):

5 מאונך: מנגנוני הצפנה שנועדו לעמוד בפני התקפות quantum (7 אותיות):

7 מאונך: תכונת בטיחות שחותכת את התעבורה כשה-VPN נופל (8 אותיות):

נקודת ביקורת 6: חיפוש מילה נסתרת

מצאו את 8 מונחי המפתח בלוח שלהלן. מילים יכולות להופיע אופקית, אנכית או באלכסון.

ג	פ	י	ח	ו	מ	ע	מ	ל	ס	ת	ע	נ	ג	ק
צ	צ	ס	ה	כ	ט	ב	ת	א	ב	ק	ג	נ	ן	כ
י	ן	ק	כ	ת	ק	י	ג	ד	ע	ו	ל	ט	ד	ח
ד	מ	ו	מ	י	ע	ס	ה	ז	ל	ו	ל	ע	פ	צ
ר	ק	ר	ק	ז	ז	ג	פ	צ	ס	נ	נ	ח	נ	פ
א	ב	פ	ש	ד	י	צ	ס	ם	ר	ט	ג	ם	י	ש
ג	ו	י	ז	ם	כ	ד	ק	א	מ	י	ד	ע	ת	ת
ר	ס	ג	ק	ב	ר	א	ה	פ	ם	ת	מ	ד	ו	כ
י	א	ד	נ	ד	ו	ה	ז	ס	ח	ד	פ	ע	ב	ל
י	ה	ח	פ	ם	ך	ד	צ	י	ה	ע	ר	ה	כ	א
ו	א	ע	נ	מ	ב	ל	ס	ו	ק	ת	ע	י	פ	פ
ו	ק	פ	ג	מ	ל	י	ן	מ	ב	ו	פ	ת	ו	ש
ט	א	פ	ם	ן	ב	פ	ן	נ	כ	ו	ח	ל	ל	ע
י	ל	ל	צ	נ	ד	ו	ז	י	ס	ע	ז	ם	א	נ
ר	ו	ר	ב	ן	פ	ת	ן	ם	ב	ז	ל	ם	ז	י

רשימת מילים

ווירגארד | ניתובכפול | זיכרוןבלבד | מתגהפסקה דליפות | אפסיומנים | פרוקסי | קוונטית

נקודת ביקורת 6 – פעילות חלופית: התאמת אוצר מילים נגישה

התאימו כל אחד מ-8 מונחי המילון מתפזורת המילים להגדרה הנכונה שלו על ידי כתיבת האות (A-H) במקום הריק.

מונחי אוצר מילים
A. ווירגארד
B. ניתובכפול
C. זיכרוןבלבד
D. מתגהפסקה
E. אפסיומנים
F. פרוקסי
G. קוונטית
H. דליפות

הגדרות ושדות התאמה
1. פרוטוקול ביניים פנימי המשמש לבידוד יישומי לקוח.
2. מנגנוני הצפנה שנועדו לעמוד בפני התקפות quantum.
3. פרוטוקול מנהור מאובטח קל משקל ובעל ביצועים גבוהים.
4. חומרת שרת עם זיכרון נדיף שאינה שומרת נתונים לאחר אתחול.
5. תכונת בטיחות שחותכת את התעבורה כשה-VPN נופל.
6. ניתוב תעבורה דרך צומת שרת כניסה וצומת שרת יציאה.
7. חשיפת יעדי שאילתות DNS מחוץ למנהרת ה-VPN.
8. תקן אי-שמירת נתונים שאומת בביקורות עצמאיות.

נקודת ביקורת 7: אתגר מילים מבולבלות

סדרו מחדש את האותיות שלהלן כדי לחשוף מושגים ומונחים מרכזיים ברשת פרטית וירטואלית (VPN). כתבו את תשובותיכם בתיבות הקלט המסופקות.

1. גריוארדי
2. ברזיודבלכ
3. אמופנמייס
4. תוטניקו
5. פביל כונות
6. קההסמפתג
7. ספקיור
8. יתדופל

פעילות בונוס: חשבו מהר

כתבו 3 תשובות לכל קטגוריה. מי שמסיים ראשון את הרשימה מנצח.

1	תכונות אבטחה ב-Mullvad		
2	שאלות לשירות הלקוחות של Mullvad		
3	דרכים ליצור סיסמה חזקה		
4	אנשים שהייתם ממליצים להם על Mullvad		
5	דברים שביקורת (audit) יכולה לבדוק		
6	מדינות הידועות בחוקי פרטיות חזקים		
7	דברים שאתם עושים באינטרנט בכל יום		
8	מדינות שתרצו בהן שרתים של Mullvad		
9	הגדרות שמפעילים לאבטחה נוספת		
10	דברים שהצפנה מגנה עליהם		
11	סוגי דליפות ב-VPN		
12	מילות אבטחה שלמדתם בדף העבודה הזה		
13	איומים ברשתות Wi-Fi ציבוריות		
14	אפליקציות שתשתמשו בהן יחד עם Mullvad		
15	מכשירים שתתקינו עליהם את Mullvad		

נקודת ביקורת 8: מקרי בוחן ב-VPN וברשתות

יישמו את המושגים שלמדתם כדי לפתור את התרחישים מהעולם האמיתי שלהלן.

מקרה בוחן 1: שילוב עמידות קוונטית

👷

תרחיש: חברה פיננסית צריכה לאבטח העברות קבצים מפני פענוח קוונטי עתידי.

שאלה לדיון: איזו תצורת מנהרה עליה לפרוס באפליקציה של Mullvad?

מקרה בוחן 2: ניתוב חשאי לצורכי תחקיר

👷

תרחיש: חוקר רוצה לנתב את הרשת שלו פעמיים כדי להסוות את נקודת הכניסה שלו.

שאלה לדיון: איזו תכונה של Mullvad יש להפעיל כדי להשיג ניתוב דרך כמה שרתים?

נקודת ביקורת 9: פענוח הצופן

מהנדס רשת מאבטח ערוצי ניתוב ומנהרות לקוח. השתמשו במפתח האותיות-למספרים שלהלן כדי לפענח את ההודעה, וכתבו את האותיות המתאימות במקומות הריקים.

מפתח הצפנה של אות למספר

א=1 ב=2 ג=3 ד=4 ה=5 ו=6 ז=7 ח=8 ט=9

י=10 כ=11 ל=12 מ=13 נ=14 ס=15 ע=16 פ=17 צ=18

ק=19 ר=20 ש=21 ת=22 ך=23 ם=24 ן=25 ף=26 ץ=27

1	12	12	6		5	13	15	10	15		1	12	12		25	6	2	21	8

12	10	10	13	10	1

ההודעה המפוענחת:

טיפ: כל מספר מייצג אות עברית אחת מהמפתח שלמעלה.

נקודת ביקורת 10: שאלות נפוצות על VPN – בסיסי (חלק A)

עיינו בשאלות והתשובות הנפוצות ביותר על רשתות פרטיות וירטואליות (VPN) ועל מנהור.

Q1: כיצד Mullvad מאבטחת חשבונות?

Mullvad משתמשת במספר חשבון שנוצר בן 16 ספרות, ללא צורך בסיסמה או באימייל. [1]

Q2: באיזה פרוטוקול Mullvad מעדיפה להשתמש?

Mullvad נותנת עדיפות ל-WireGuard בזכות המהירות, הפשטות וההצפנה המודרנית שלו. [9]

Q3: האם שרתי Mullvad עוברים ביקורת?

כן, חברות אבטחה חיצוניות מבצעות באופן קבוע ביקורות תשתית וקוד.

Q4: האם Mullvad תומכת ב-OpenVPN?

לא, Mullvad הסירה את OpenVPN ב-15 בינואר 2026; היא תומכת רק ב-WireGuard. [7]

Q5: מהו ה-kill switch של Mullvad?

זהו כלל חומת אש משולב שמונע תעבורת אינטרנט אם ה-VPN נכשל.

נקודת ביקורת 10: שאלות נפוצות על VPN – בסיסי (חלק B)

עיינו בשאלות והתשובות הנפוצות ביותר על רשתות פרטיות וירטואליות (VPN) ועל מנהור.

Q6: האם Mullvad תומכת ב-IPv6?

כן, Mullvad תומכת בניתוב IPv6 מקורי ובהגנה מפני דליפות.

Q7: האם Mullvad מציעה multihop?

כן, WireGuard multihop מאפשר שרשור של כמה מיקומי שרתים.

Q8: האם אפשר להשתמש בפותרי DNS מותאמים אישית?

כן, ניתן להגדיר כתובות DNS מותאמות אישית בהגדרות הלקוח של Mullvad.

Q9: כיצד מונעים יומנים?

תצורות מערכת משביתות רישום ומנקות מטמונים בכל דמוני השרת.

Q10: היכן Mullvad מאוגדת?

Mullvad התאגדה ביוטבורג שבשוודיה, תחת תחום השיפוט השוודי.

נקודת ביקורת 10: שאלות נפוצות על VPN – מתקדם (חלק C)

חקרו היבטים טכניים מתקדמים של פרוטוקולי מנהור VPN, שילובי לקוחות לנייד ופריסה ארגונית.

Q1: כיצד פועלת רוטציית מפתחות?

האפליקציה מחליפה מפתחות WireGuard באופן אוטומטי; מרווח ברירת המחדל ב-CLI הוא 30 ימים. [3]

Q2: מהן מנהרות עמידות לקוונטים?

הם מוסיפים ל-WireGuard החלפת מפתחות ML-KEM ו-Classic McEliece כדי לעמוד בפני התקפות קוונטיות עתידיות. [2]

Q3: כיצד שרתי RAM בלבד מאובטחים?

צמתים אלה אינם כותבים נתונים לכוננים קשיחים, ולכן גניבת שרתים פיזיים חסרת תועלת.

Q4: מהי פונקציית פרוקסי SOCKS5?

הוא עוזר לנתב תעבורה של אפליקציות מסוימות בתוך המנהרה ומונע דליפות לרשתות חיצוניות.

Q5: האם Mullvad מגינה מפני דליפות WebRTC?

כן, האפליקציה מכריחה שאילתות WebRTC לעבור דרך ממשק ה-VPN כדי להגן על כתובות IP מקומיות.

נקודת ביקורת 10: שאלות נפוצות על VPN – מתקדם (חלק D)

חקרו היבטים טכניים מתקדמים של פרוטוקולי מנהור VPN, שילובי לקוחות לנייד ופריסה ארגונית.

Q6: כיצד Mullvad מטפלת בפשיטות משטרה?

ל-Mullvad אין יומנים של מסד נתוני משתמשים, כלומר לא ניתן לחלץ מידע על משתמשים.

Q7: מהו סיכון סמכות השיפוט של שוודיה?

שוודיה היא חברה ב-14 Eyes, אך ארכיטקטורת אפס היומנים של Mullvad מסירה את סיכון הנתונים.

Q8: האם ביקורות אפליקציות הלקוח הן בקוד פתוח?

כן, האפליקציות הן קוד פתוח (GPL-3) ונבדקות על ידי חברות כמו X41 D-Sec. [6].

Q9: כיצד פועל split tunneling?

הוא משתמש בטבלאות הניתוב של מערכת ההפעלה כדי להוציא אפליקציות מסוימות מתקורת ה-VPN.

Q10: כיצד Mullvad מטפלת בתשלומים במזומן?

המזומן נשלח בדואר עם קוד אסימון, מזוכה ידנית, והמעטפות נגרסות.

חלק 11: 10 עובדות ותובנות מהעולם האמיתי על VPN

עיינו בעובדות מהעולם האמיתי על מהירויות הצפנה ב-VPN, ביקורות פרוטוקולים, קישוריות בנייד ועבודה מרחוק בארגונים.

1. תובנות על VPN

Mullvad נוסדה ב-2009 בידי Amagicom AB ביוטבורג שבשוודיה.

2. תובנות על VPN

מספרי חשבון הם המזהה היחיד המשמש לזיכוי חשבונות ולגישה אליהם.

3. תובנות על VPN

לא נשמרים שמות, כתובות אימייל, סיסמאות או מספרי טלפון במסד נתוני המשתמשים.

4. תובנות על VPN

מפתחות WireGuard נוצרים מקומית במכשירי הלקוח כדי למנוע פגיעה בצד השרת.

5. תובנות על VPN

ביקורת התשתית של Cure53 מ-2024 לא מצאה פגם הפוגע באנונימיות תעבורת ה-VPN. [5]

6. תובנות על VPN

בכל שרת WireGuard של Mullvad פועל פרוקסי SOCKS5, הנגיש רק בתוך המנהרה. [8]

7. תובנה על VPN

ניתן להסוות תעבורת WireGuard באמצעות Shadowsocks, QUIC או LWO כדי לעבור חומות אש. [10]

8. תובנה על VPN

Mullvad השלימה את המעבר לשרתי VPN הפועלים ב-RAM בלבד בספטמבר 2023. [4]

9. תובנה על VPN

ML-KEM ו-Classic McEliece מנהלים משא ומתן על מפתח משותף מראש עמיד לקוונטים עבור WireGuard. [2]

10. תובנות על VPN

מעטפות המזומן ותכולתן שאינה כסף נגרסות לאחר שהזמן מזוכה.

מקורות והפניות טכניים

מדריך הלימוד והפאזלים האינטראקטיביים נערכו על סמך תקנים טכניים, מפרטים ומסגרות רגולטוריות גלובליים.

מקורות אקדמיים ותעשייתיים

[1] Mullvad VPN. (n.d.). Why Mullvad VPN?
https://mullvad.net/en/why-mullvad-vpn

[2] Mullvad VPN. (n.d.). Quantum-resistant tunnels with WireGuard.
https://mullvad.net/en/help/quantum-resistant-tunnels-with-wireguard

[3] Mullvad VPN. (n.d.). CLI commands for using WireGuard.
https://mullvad.net/en/help/cli-command-wg

[4] Mullvad VPN. (2023). We have successfully completed our migration to RAM-only VPN infrastructure.
https://mullvad.net/en/blog/we-have-successfully-completed-our-migration-to-ram-only-vpn-infrastructure

[5] Mullvad VPN. (2024). Fourth Infrastructure audit completed by Cure53.
https://mullvad.net/en/blog/fourth-infrastructure-audit-completed-by-cure53

[6] Mullvad VPN. (2024). The report for the 2024 security audit of the app is now available.
https://mullvad.net/en/blog/the-report-for-the-2024-security-audit-of-the-app-is-now-available

[7] Mullvad VPN. (2024). Removing OpenVPN 15th January 2026.
https://mullvad.net/en/blog/removing-openvpn-15th-january-2026

[8] Mullvad VPN. (n.d.). SOCKS5 proxy.
https://mullvad.net/en/help/socks5-proxy

[9] Mullvad VPN. (n.d.). Why WireGuard?
https://mullvad.net/en/help/why-wireguard

[10] Mullvad VPN. (n.d.). Using Mullvad VPN in restrictive locations.
https://mullvad.net/en/help/connecting-to-mullvad-vpn-from-restrictive-locations

[11] National Institute of Standards and Technology. (2024). FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard.
https://csrc.nist.gov/pubs/fips/203/final

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

מפתח תשובות: נקודת ביקורת 1 – שאלות אמריקאיות

1 שאלה 1

תשובה נכונה: B

הערה למורה

איזה פרוטוקול מנהור הוא ברירת המחדל באפליקציה של Mullvad? → WireGuard

2 שאלה 2

תשובה נכונה: A

הערה למורה

לחיצה על "generate account" נותנת מספר חשבון; לא מתבקשים אימייל או מידע אישי אחר.

3 שאלה 3

תשובה נכונה: B

הערה למורה

מנהרות WireGuard העמידות לקוונטים של Mullvad משתמשות ב-ML-KEM וב-Classic McEliece כדי להסכים על מפתח משותף מראש (preshared key). [1].

4 שאלה 4

תשובה נכונה: C

הערה למורה

איזה מנגנון אבטחה חוסם סכנות של דליפות WebRTC? → ניתוב WebRTC דרך ממשק ה-VPN

5 שאלה 5

תשובה נכונה: B

הערה למורה

איזו תכונת multihop מנתבת תעבורה דרך כמה צמתים? → WireGuard Multihop

מפתח תשובות: נקודת ביקורת 2 – נכון או לא נכון

6 **שאלה 6**

תשובה נכונה: לא נכון

הערה למורה

לא נכון: Mullvad לעולם אינה מבקשת אימייל; חשבונות מזוהים רק באמצעות מספר שנוצר.

7 **שאלה 7**

תשובה נכונה: נכון

הערה למורה

אפשר להגדיר פרוקסי SOCKS5 בתוך מנהרות Mullvad.

8 **שאלה 8**

תשובה נכונה: לא נכון

הערה למורה

לא נכון: Mullvad מחזיקה בבעלותה חלק מהשרתים אך גם שוכרת שרתים ייעודיים מספקים.

9 **שאלה 9**

תשובה נכונה: נכון

הערה למורה

מתג הקטיעה של הרשת פעיל תמיד כברירת מחדל.

10 **שאלה 10**

תשובה נכונה: נכון

הערה למורה

תשלומים במזומן שנשלחו בדואר אינם ניתנים להחזר כלל.

מפתחות אוצר מילים ומחוון הערכה

מחוון הערכה למורה: תנו 1 נקודה לכל התאמה נכונה (סה"כ 8 נקודות) ולכל מונח הקשר (סה"כ 8 נקודות).

נקודת ביקורת 4: מפתח תשובות – התאמת מושגים

B 1. ווירגארד	D 2. ניתוב כפול	G 3. RAM בלבד	A 4. מתג הפסקה
H 5. אפס יומנים	C 6. פרוקסי	E 7. קוונטית	F 8. דליפות

נקודת ביקורת 3: מפתח תשובות – מונחי מפתח

1 ווירגארד	2 ניתוב כפול	3 זיכרון בלבד	4 מתג הפסקה
5 אפס יומנים	6 פרוקסי	7 קוונטית	8 דליפות

נקודת ביקורת 6 – פעילות חלופית: מפתח תשובות – התאמת אוצר מילים

1 F – פרוקסי	2 G – קוונטית	3 A – ווירגארד	4 C – זיכרוןבלבד
5 D – מתגהפסקה	6 B – ניתובכפול	7 H – דליפות	8 E – אפסיומנים

הערות לדיון עבור מורים

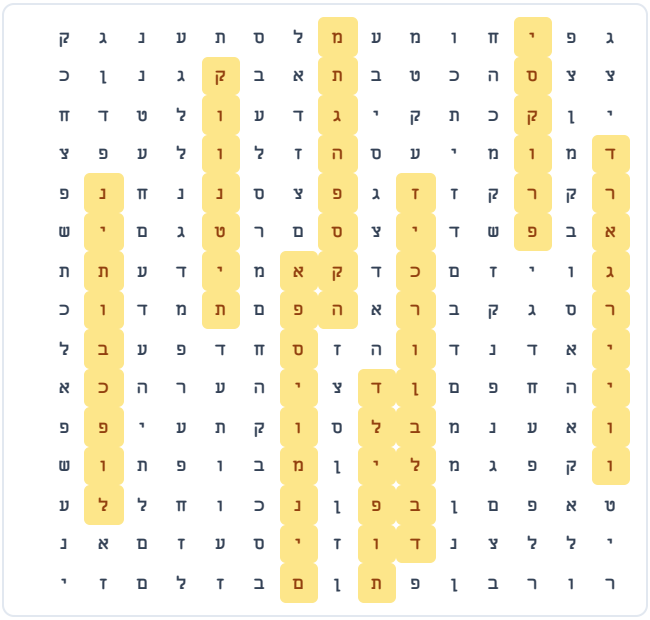
מונחי מפתח:
ודאו שהתלמידים מסבירים במילים שלהם את ווירגארד, ניתוב כפול ו-RAM בלבד ונותנים דוגמה לכל אחד מהם.

מקרי בוחן:
בקשו מהתלמידים לבסס את ההמלצות שלהם על עובדות מדף העבודה ולא על דעות.

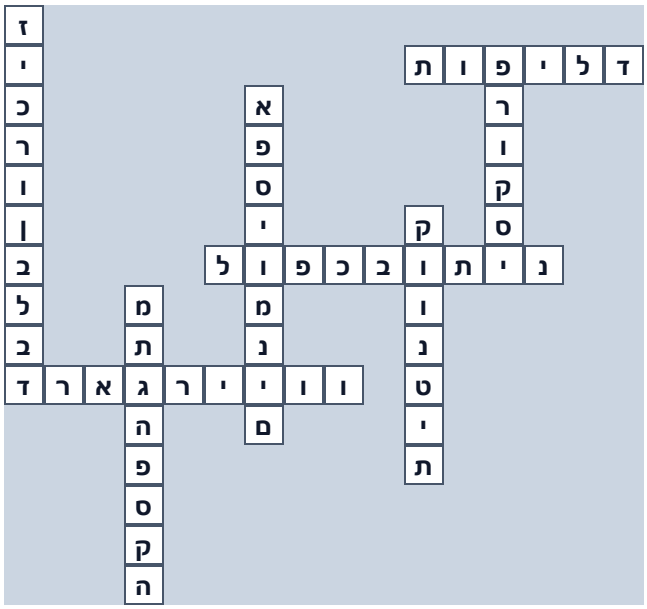
הערכת מקורות:
בקשו מהתלמידים לאמת לפחות טענה אחת במקורות של דף העבודה, ודונו מדוע נתונים, מחירים וכללים עשויים להשתנות עם הזמן.

מפתחות פאזלים והערות למורה

פתרון תפזורת



פתרון תשבץ



מדריך למורה לפתרונות התשבץ

מאוזן

2 מאוזן: דליפות חשיפת יעדי שאילתות DNS מחוץ למנהרת ה-VPN (6 אותיות)

6 מאוזן: ניתובכפול ניתוב תעבורה דרך צומת שרת כניסה וצומת שרת יציאה (9 אותיות)

8 מאוזן: ווירגארד פרוטוקול מנהור מאובטח קל משקל ובעל ביצועים גבוהים (9 אותיות)

מאונך

1 מאונך: זיכרוןבלבד חומרת שרת עם זיכרון נדיף שאינה שומרת נתונים לאחר אתחול (10 אותיות)

3 מאונך: פרוקסי פרוטוקול ביניים פנימי המשמש לבידוד יישומי לקוח (6 אותיות)

4 מאונך: אפסיומנים תקן אי-שמירת נתונים שאומת בביקורות עצמאיות (9 אותיות)

5 מאונך: קוונטית מנגנוני הצפנה שנועדו לעמוד בפני התקפות quantum (7 אותיות)

7 מאונך: מתגהפסקה תכונת בטיחות שחותכת את התעבורה כשה-VPN נופל (8 אותיות)

מפתח פתרונות: מילים מבולבלות ופענוח הצופן

מפתח הערכה לפעילות פענוח מילות אוצר המילים ולאתגר הצופן הסודי.

מפתח פענוח מילים מבולבלות

1. גריווארדי — ווירגארד
2. ברזיודבלק — זיכרונבלבד
3. אמופנמייס — אפסיומנים
4. תוטניקו — קוונטית
5. פבילכונות — ניתובכפול
6. קההסמפתג — מתגהפסקה
7. ספקיור — פרוקסי
8. יתדופל — דליפות

מפתח אתגר הצופן הסודי

"חשבון ללא סיסמה וללא אימייל"

מפתח תשובות למקרי הבוחן

A מקרה בוחן 1: שילוב עמידות קוונטית

פתרון למורה

הנחיות הערכה

תשובות התלמידים צריכות לכלול את הנקודות הבאות:

- ניתוח תרחיש: חברה פיננסית צריכה לאבטח העברות קבצים מפני פענוח קוונטי עתידי.
- אסטרטגיה ופתרון מומלצים: פרסו מנהרות WireGuard עמידות לקוונטים באמצעות מפתחות משותפים מראש פוסט-קוונטיים.

B מקרה בוחן 2: ניתוב חשאי לצורכי תחקיר

פתרון למורה

הנחיות הערכה

תשובות התלמידים צריכות לכלול את הנקודות הבאות:

- ניתוח תרחיש: חוקר רוצה לנתב את הרשת שלו בניתוב כפול כדי להסוות את נקודת הכניסה שלו.
- אסטרטגיה ופתרון מומלצים: הפעילו את תכונת WireGuard Multihop של Mullvad כדי לשרשר צמתי כניסה ויציאה.