שם: _____ תאריך: _____ ציון: _____

כיצד לבחור VPN
דף עבודה

הערכת ספקי VPN, תקני אבטחה, ביקורות ומדיניות רישום

סקירת למידה: VPN

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 העקרונות הבסיסיים של רשתות וירטואליות פרטיות (VPN). תחקרו כיצד מנהרות מוצפנות מאבטחות את הנתונים שלכם, כיצד פועלים פרוטוקולי רשת וכיצד לזהות ולצמצם דליפות פרטיות.

נקודות הביקורת בדף העבודה

- [ ] **חלק 1-4: שלטו במושגים ובפרוטוקולים של VPN.**
- [ ] **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 של VPN.com

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

מפת הלמידה שלכם: VPN

- העריכו את השיפוט של הספק ואת מדיניות אי-שמירת הרישומים לצורכי פרטיות.
- השוו פרוטוקולי מנהור כמו WireGuard ו-OpenVPN מבחינת מהירות.
- נתחו תכונות אבטחה כמו מתגי חירום וצמתי שרת מסוג RAM בלבד.
- זהו ביקורות אבטחה עצמאיות ותוכניות תמחור בעת הבחירה.
- בחרו מיקומי שרתים בהתאם לצורכי המהירות ושחרור החסימות הגיאוגרפיות שלכם.

הוראות דף עבודה לבחירה

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 בחירת תשתית VPN מאובטחת. ולסיום, פעילות הבונוס "חשבו מהר".

בחירת VPN (מבוא)

בחירת ה-VPN המתאים דורשת להסתכל מעבר להייפ שיווקי. ספק אמין חייב להפעיל מדיניות אפס רישום מוכחת, פרוטוקולי הצפנה מאובטחים ולקוחות בקוד פתוח. באמצעות הערכת תכונות אבטחה, סמכויות שיפוט וביצועי מהירות תוכלו לבחור VPN שמתאים לצורכי ההגנה הדיגיטלית שלכם.

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

נקודת ביקורת 1: אתגר שאלות אמריקאיות

1. מהו הגורם המרכזי בבחירת ספק VPN מאובטח?

- A. מספר מדינות השרתים
- B. מדיניות no-logs שנבדקה בביקורת עצמאית
- C. דרגת המחיר החודשית הנמוכה ביותר
- D. חסויות פרסום מרהיבות

2. איזה פרוטוקול VPN מציע את האיזון הטוב ביותר בין מהירות לאפשרות ביקורת?

- A. PPTP (ישן)
- B. L2TP/IPSec
- C. OpenVPN ב-TCP בלבד
- D. WireGuard

3. מדוע על משתמשים להימנע מ-VPN חינמיים לפעילויות רגישות?

- A. הן אסורות בארצות הברית
- B. הם מוכרים לעיתים קרובות את היסטוריית הגלישה שלכם
- C. הם אינם תומכים בגלישה בסיסית באינטרנט
- D. הם דורשים חומרה מיוחדת כדי להתחבר

4. מה קובעת סמכות השיפוט המשפטית של מדינת הבית של ספק?

- A. מהירות חיבור השרת
- B. סוגי המכשירים הנתמכים
- C. חוקים מקומיים הנוגעים לשמירת נתונים ולצווי חיפוש
- D. ערכת הנושא החזותית של אפליקציית הלקוח

5. מהי המטרה העיקרית של תכונת ה-"kill switch" בלקוח VPN?

- A. כדי לחסום גישה לאינטרנט אם חיבור ה-VPN נופל
- B. כדי למחוק את כל האפליקציות המותקנות במכשיר
- C. כדי להכפיל את מהירות החיבור לשרת
- D. כדי להפעיל מחדש את מערכת ההפעלה כשהיא לא פעילה

נקודת ביקורת 2: אתגר נכון או לא נכון

שאלה 6

6. VPN מגן על המכשיר שלך מפני הורדות נוזקות וקובצי וירוס.

נכון לא נכון

שאלה 7

7. ביקורות עצמאיות של חברות כמו Deloitte מאמתות טענות על אי-רישום.

נכון לא נכון

שאלה 8

8. חוקי מדינת הבית של הספק אינם משפיעים על פרטיות נתוני המשתמש.

נכון לא נכון

שאלה 9

9. קל יותר לבדוק את בסיס הקוד הקומפקטי של WireGuard מאשר את זה של OpenVPN.

נכון לא נכון

שאלה 10

10. שירותי VPN חינמיים מוכרים לעיתים קרובות פרסומות או עוקבים אחר משתמשים כדי לכסות את עלויות השרתים.

נכון לא נכון

נקודת ביקורת 3: השלמת מונחי מפתח

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

1. מדיניות _____ מאומתת באופן עצמאי מחייבת ספק VPN שלא לתעד את היסטוריית הגלישה שלך.
2. הפרוטוקול המודרני _____ מספק מהירות גבוהה ובסיס קוד קטן מאוד.
3. תכונת בטיחות בשם _____ עוצרת את כל התעבורה אם חיבור ה-VPN נכשל פתאום.
4. בחינת _____ של הספק קובעת אם הוא כפוף להסכמי מעקב.
5. אבטחת שרתים באמצעות דיסקים מסוג _____ עוזרת למנוע שמירת נתוני משתמש לאחר אתחול.
6. אימות טענות של אפס ידע מחייב _____ אבטחה של צד שלישי מחברות מהימנות.

בנק מילים

אפס יומנים | ביקורת | וויירגארד | זיכרון בלבד | חינמי | מתג הפסקה | סמכות שיפוט | קוד פתוח

כתבו את תשובותיכם כאן:

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

נקודת ביקורת 4: התאמת מושגים ברשתות

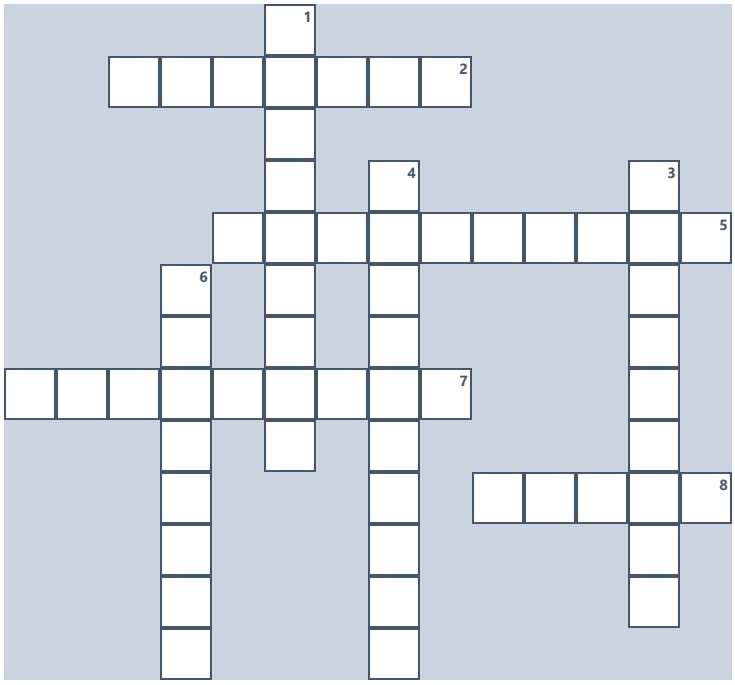
התאמת הגדרות

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

1. WireGuard	A	שירות חיבור בסיכון גבוה שמרוויח לעיתים קרובות מרישום ומכירה של נתוני גלישה.
2. יומנים מבוקרים	B	מנגנון בטיחות החוסם ניתוב אינטרנט אם המנהרה המאובטחת מתנתקת.
3. שיפוט	C	ברית בינלאומית לשיתוף מודיעין בין ארה"ב, בריטניה, קנדה, אוסטרליה וניו זילנד.
4. מתג חירום (Kill Switch)	D	תשתית חומרה שפועלת על זיכרון נדיף, ולכן הנתונים אינם נשמרים בדיסק.
5. Five Eyes	E	האזור הגאוגרפי השולט בחובות המשפטיות של ספק ה-VPN.
6. VPN חינמי	F	פרוטוקול מודרני ומהיר המשתמש בכ-4,000 שורות קוד הניתנות לביקורת בקלות רבה.
7. שרתי RAM בלבד	G	פרוטוקול בוגר בקוד פתוח שנבדק רבות, עם בסיס קוד גדול בהרבה מזה של WireGuard.
8. OpenVPN	H	טענת פרטיות שאומתה על ידי חברות אבטחת סייבר עצמאיות של צד שלישי.

נקודת ביקורת 5: תשבץ

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



מאוזן

2. פרוטוקול בוגר ומבוקר רבות, עם בסיס קוד גדול בהרבה מזה של (7) WireGuard

5. האזור הגאוגרפי השולט בהתחייבויות המשפטיות של ספק ה-(10) VPN

7. פרוטוקול מודרני ומהיר המבוסס על כ-4,000 שורות קוד הניתנות לביקורת בקלות (9)

8. שירות חיבור בסיכון גבוה שלעתים מרוויח מתיעוד ומכירה של נתוני גלישה (5)

מאונך

1. טענת פרטיות שאומתה על ידי חברות אבטחת סייבר עצמאיות של צד שלישי (9)

3. ברית שיתוף מודיעין בינלאומית בין ארה״ב, בריטניה, קנדה, אוסטרליה וניו זילנד (9)

4. תשתית חומרה הפועלת כולה על זיכרון נדיף ומונעת אחסון נתונים (10)

6. מנגנון בטיחות החוסם ניתוב אינטרנט אם המנהרה המאובטחת מתנתקת (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: פרוטוקול בוגר ומבוקר רבות, עם בסיס קוד גדול בהרבה מזה של WireGuard (7 אותיות):

5 מאוזן: האזור הגאוגרפי השולט בהתחייבויות המשפטיות של ספק ה-VPN (10 אותיות):

7 מאוזן: פרוטוקול מודרני ומהיר המבוסס על כ-4,000 שורות קוד הניתנות לביקורת בקלות (9 אותיות):

8 מאוזן: שירות חיבור בסיכון גבוה שלעתים מרוויח מתיעוד ומכירה של נתוני גלישה (5 אותיות):

מאונך

1 מאונך: טענת פרטיות שאומתה על ידי חברות אבטחת סייבר עצמאיות של צד שלישי (9 אותיות):

3 מאונך: ברית שיתוף מודיעין בינלאומית בין ארה״ב, בריטניה, קנדה, אוסטרליה וניו זילנד (9 אותיות):

4 מאונך: תשתית חומרה הפועלת כולה על זיכרון נדיף ומונעת אחסון נתונים (10 אותיות):

6 מאונך: מנגנון בטיחות החוסם ניתוב אינטרנט אם המנהרה המאובטחת מתנתקת (8 אותיות):

נקודת ביקורת 6: חיפוש מילה נסתרת

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

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

רשימת מילים

ווירגארד, אפסיומנים, סמכותשיפוט, מתגהפסקה קודפתוח, חמשעיניים, חינמי, זיכרוןבלבד

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. אפסיומנים
C. סמכותשיפוט
D. מתגהפסקה
E. חמשעיניים
F. חינמי
G. זיכרוןבלבד
H. קודפתוח

הגדרות ושדות התאמה	
1. ברית שיתוף מודיעין בינלאומית בין ארה״ב, בריטניה, קנדה, אוסטרליה וניו זילנד.	
2. פרוטוקול מודרני ומהיר המבוסס על כ-4,000 שורות קוד הניתנות לביקורת בקלות.	
3. פרוטוקול בוגר ומבוקר רבות, עם בסיס קוד גדול בהרבה מזה של WireGuard.	
4. שירות חיבור בסיכון גבוה שלעתים מרוויח מתיעוד ומכירה של נתוני גלישה.	
5. מנגנון בטיחות החוסם ניתוב אינטרנט אם המנהרה המאובטחת מתנתקת.	
6. תשתית חומרה הפועלת כולה על זיכרון נדיף ומונעת אחסון נתונים.	
7. האזור הגאוגרפי השולט בהתחייבויות המשפטיות של ספק ה-VPN.	
8. טענת פרטיות שאומתה על ידי חברות אבטחת סייבר עצמאיות של צד שלישי.	

נקודת ביקורת 7: אתגר מילים מבולבלות

סדרו מחדש את האותיות שלהלן כדי לחשוף מושגים ומונחים מרכזיים ב-VPN. כתבו את תשובותיכם בתיבות הקלט הניתנות למילוי.

1. גריוואדרי
2. ווסמתטיפשכ
3. חנימיסעיש
4. ובודרלבזיכ
5. נופממיאיס
6. קההסמפתג
7. מיחני
8. ופחקותד

פעילות בונוס: חשבו מהר

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

1. דברים ש-VPN יכול להסתיר
2. דברים שחשובים יותר ממחיר
3. מקומות לקרוא בהם ביקורות על VPN
4. דברים ש-VPN לא יכול להגן עליכם מפניהם
5. שאלות לצוות המכירות של VPN
6. דברים שספק האינטרנט שלכם יכול לראות
7. פריטים ברשימת הבדיקה שלכם בבחירת VPN
8. מקומות שבהם תשתמשו ב-VPN
9. סימני אזהרה אצל ספק VPN
10. מילים הקשורות לפרטיות
11. דברים שהייתם בודקים קודם
12. הבטחות שספק VPN טוב מבטיח
13. סיבות להשתמש ב-VPN בזמן נסיעות
14. מכשירים שיכולים להשתמש ב-VPN
15. מיתוסים על VPN

נקודת ביקורת 8: מקרי בוחן ב-VPN

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

שרה (סטודנטית בבית קפה)

👩‍💻 "היי! אני יושבת ב-Coffee & Bytes. יש שם רשת ציבורית לא מאובטחת בשם 'Free_Wi-Fi_No_Password'. אני רוצה להיכנס לאימייל של בית הספר ולהעלות את העבודה שלי, אבל אני חוששת מהאקרים. מהם הסיכונים בשימוש ברשת הזו בלי VPN, וכיצד VPN מאבטח את הנתונים שלי?"

אלכס (סטודנט נוסע)

👨‍💻 "אוי לא! אני מטייל בחו״ל בשביל פרויקט ומנסה לצפות בסרט תיעודי על ביולוגיה המתארח בשרת במדינה שלי. אבל האתר אומר 'הסרטון הזה אינו זמין במיקומך הנוכחי.' למה אני חסום, וכיצד VPN יכול לעזור לי לצפות בו?"

נקודת ביקורת 9: פענוח הצופן

כדי להשלים את אימון מדריך הבחירה שלכם, פענחו את ההודעה הנסתרת הזו על בחירת תשתית מאובטחת.

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

22	11	20	16	13		24	16		22	6	8	6	4		6	6	21	5

22	8	9	2	6	1	13

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 שיש ללקוחות פוטנציאליים על שימוש ברשתות פרטיות וירטואליות.

Q1: מהו VPN וכיצד הוא פועל?

רשת וירטואלית פרטית (VPN) מצפינה את חיבור האינטרנט שלך ומנתבת את התעבורה שלך דרך שרת מרוחק מאובטח. כך מוסתרת כתובת ה-IP הציבורית שלך, ומוגבל מה שמשקיפים ברשת המקומית וספק האינטרנט שלך יכולים לראות לגבי תעבורה שמנותבת דרך מנהרת ה-VPN.

Q2: מדוע כדאי להשתמש ב-VPN?

VPN מגן על הפרטיות הדיגיטלית שלך, מאבטח את החיבור שלך ברשתות Wi-Fi ציבוריות (כמו בבתי קפה או בשדות תעופה), עשוי להפחית האטה מבוססת פעילות כאשר ספק האינטרנט אינו יכול לזהות את סוג התעבורה המוצפנת, עוקף הגבלות גיאוגרפיות כדי לגשת לתוכן גלובלי ומסייע באבטחת משאבי עבודה מרחוק.

Q3: האם VPN הופך אותי לאנונימי לחלוטין ברשת?

לא. אף שה-VPN מסתיר את כתובת ה-IP שלכם ומצפין תעבורה, עדיין ניתן לעקוב אחריכם באמצעות עוגיות דפדפן, חשבונות פעילים (כמו Google או Facebook), טביעת אצבע דיגיטלית של הדפדפן, או אם ספק ה-VPN שלכם רושם את הנתונים שלכם.

Q4: האם VPN יאט את מהירות האינטרנט שלי?

כן, במעט. תהליך ההצפנה והמרחק הפיזי לשרת ה-VPN מוסיפים זמן השהיה ועומס נוסף. ההשפעה משתנה לפי הספק, הפרוטוקול, מרחק השרת, המכשיר ותנאי הרשת.

Q5: כיצד הוא מרוויח כסף?

בדקו את המודל העסקי. מנויים, שכבות Freemium ומכירת נתונים משפיעים כולם על מידת האמון שתוכלו לתת ב-VPN, ושירות שאינו אוסף את הנתונים שלכם לעולם אינו יכול למכור אותם. קראו תחילה את מדיניות הפרטיות. [1]

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

עיינו בשאלות והתשובות הנפוצות ביותר שיש ללקוחות פוטנציאליים על שימוש ברשתות פרטיות וירטואליות.

Q6: האם אפשר להשתמש ב-VPN חינמי?

שירותי VPN חינמיים עשויים להסתמך על פרסום, פיצ׳רים מוגבלים, ניתוח שימוש, מכסות נתונים או מודלים אחרים של מונטיזציה. מומלץ לעיין במדיניות הפרטיות של הספק, בבעלות עליו, בביקורות ובמודל העסקי שלו לפני השימוש.

Q7: מהי מדיניות "no-logs"?

מדיניות אי-רישום מתארת אילו נתוני פעילות וחיבור הספק טוען שאינו שומר. ההיקף המדויק משתנה, ולכן על הקוראים לעיין במדיניות ובממצאי הביקורת העצמאית.

Q8: כיצד בוחרים את ה-VPN הטוב ביותר?

חפשו מדיניות אי-רישום שעברה ביקורת, פרוטוקולים חזקים (WireGuard, OpenVPN), מיקומי שרתים מאובטחים, מהירויות גבוהות, שרתים הפועלים ב-RAM בלבד, תכונת מתג חירום (kill switch) ותחום שיפוט מחוץ לבריתות לשיתוף מודיעין (כמו 5/9/14 Eyes).

Q9: האם אפשר להשתמש ב-VPN בטלפון ובטלוויזיה החכמה שלי?

כן. ספקי VPN מודרניים מציעים אפליקציות ייעודיות ל-Linux, Windows, macOS, Android, iOS וטלוויזיות חכמות, וכן הגדרות לנתבים כדי להגן על כל המכשירים ברשת הביתית.

Q10: מהו Kill Switch?

מתג חירום (Kill Switch) הוא תכונת אבטחה שמנתקת אוטומטית את המכשיר שלך מהאינטרנט אם חיבור ה-VPN נופל. כך נמנעת דליפה של הנתונים הלא מוצפנים או של כתובת ה-IP האמיתית שלך.

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

חקרו היבטים טכניים ומבניים של רשתות וירטואליות פרטיות ופרוטוקולי מנהור מאובטחים.

Q1: מה ההבדל בין WireGuard, OpenVPN ו-IKEv2?

WireGuard הוא פרוטוקול מודרני וקל משקל (כ-4,000 שורות קוד בלבד) המציע מהירויות גבוהות וזמני חיבור קצרים. OpenVPN הוא פרוטוקול קוד-פתוח מאובטח מאוד ומנוסה בשטח. IKEv2 מצוין למכשירים ניידים בזכות יכולתו להתחבר מחדש במהירות בעת מעבר בין רשתות.

Q2: מהו ניתוב VPN כפול או Multi-Hop?

Multi-Hop מנתב את התעבורה שלכם דרך שני שרתי VPN או יותר ברצף. כך נוספת שכבת הצפנה שנייה, ואם שרת אחד נפרץ היא מסייעת להסתיר את כתובת ה-IP האמיתית שלכם מהקפיצה השנייה.

Q3: מהו WebRTC leaking וכיצד VPN מונע אותו?

WebRTC הוא פרוטוקול דפדפן שיכול לחשוף את כתובות ה-IP המקומית והציבורית האמיתיות שלכם גם כש-VPN פעיל. שירותי VPN מובילים חוסמים או מזייפים בקשות WebRTC באפליקציות לשולחן העבודה ולנייד ובתוספי הדפדפן.

Q4: מהם שרתי RAM בלבד ומדוע הם חשובים?

שרתים מסורתיים כותבים נתונים לכוננים קשיחים, שניתן לתפוס או לפרוץ. שרתי RAM בלבד (ללא דיסקים) פועלים כולם בזיכרון נדיף (RAM). כאשר השרת מאותחל מחדש או כבוי, הנתונים המוחזקים בזיכרון נמחקים.

Q5: כיצד הסוואה (Obfuscation) עוקפת חסימות VPN?

ערפול (או "Stealth VPN") מסווה את חבילות תעבורת ה-VPN כך שייראו כתעבורת רשת HTTPS רגילה (פורט 443). כך קל יותר לעקוף את בדיקת החבילות העמוקה (DPI) שבה משתמשות ממשלות או רשתות של בתי ספר ומשרדים כדי לחסום VPN.

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

חקרו היבטים טכניים ומבניים של רשתות וירטואליות פרטיות ופרוטוקולי מנהור מאובטחים.

Q6: מהו Split Tunneling ומתי כדאי להשתמש בו?

Split Tunneling מאפשר לכם לבחור אילו אפליקציות מנותבות דרך מנהרת ה-VPN המוצפנת ואילו מתחברות ישירות לאינטרנט. השתמשו בו כדי לנתב אפליקציות בנקאות רגישות דרך ה-VPN בעוד משחקים מקומיים מתחברים ישירות, וכך להימנע מההשהיה שה-VPN מוסיף.

Q7: כיצד פועלת סודיות מתקדמת (Perfect Forward Secrecy)?

PFS מבטיח שייווצר מפתח הצפנה ייחודי וזמני לכל הפעלה. גם אם מפתח פרטי ייחשף בעתיד, לא ניתן להשתמש בו כדי לפענח הפעלות קודמות או עתידיות, משום שהן השתמשו במפתחות בלתי תלויים.

Q8: מהם בריתות 5/9/14 Eyes ומדוע זה צריך לעניין אותי?

השיפוט יכול להשפיע על ההליך המשפטי שספק עשוי להתמודד איתו, אך סיכון הפרטיות המעשי תלוי גם באילו נתונים הספק שומר, בארכיטקטורה הטכנית שלו, בבעלות, בדוחות שקיפות ובהיסטוריית הביקורות.

Q9: מהי הגנה מפני דליפות DNS?

הגנה מפני דליפות DNS מכריחה את המכשיר שלכם לשלוח שאילתות חיפוש של אתרים (שאילתות DNS) דרך שרתי ה-DNS הפרטיים והמוצפנים של ה-VPN במקום דרך השרתים של ספק האינטרנט שלכם. כך ספק האינטרנט לא יכול לעקוב אחרי האתרים שבהם אתם מבקרים.

Q10: מדוע כדאי לבדוק מי מפעיל ומאשר VPN?

המוניטין חשוב. חקרו את בעלי החברה ומנהליה, חפשו ביקורות ציבוריות של צד שלישי ובדקו מה אומרים מומחי אבטחה עצמאיים והעיתונות לפני שאתם סומכים עליה. [1]

חלק 11: 10 עובדות מעניינות על VPN ותובנות מהעולם האמיתי

עיינו בעובדות ובתובנות רבות ערך מהעולם האמיתי על ההיסטוריה, השוק והטכנולוגיה של VPN.

1. פרוטוקול ה-VPN הראשון

PPTP (Point-to-Point Tunneling Protocol), פרוטוקול VPN מוקדם של קבוצה בהובלת Microsoft בשנות ה-1990, נחשב כיום לבלתי מאובטח, ולכן VPN מודרניים משתמשים ב-WireGuard או ב-OpenVPN. [1]

2. הערכת שווי שוק

שוק ה-VPN העולמי חווה צמיחה מהירה, המונעת מדרישות עבודה מרחוק גוברות וצורכי אבטחה ארגוניים.

3. מהפכת WIREGUARD

ל-WireGuard בסיס קוד יעיל ומצומצם מאוד שנועד ליעילות, מה שמקל לבדוק אותו לאיתור פגיעויות אבטחה בהשוואה לפרוטוקולים מסורתיים. [3]

4. תקני ביקורת מחמירים

ספקי VPN מובילים שוכרים חברות כמו Deloitte, KPMG או PwC לבדיקת טענות אי-שמירת היומנים, וחברות אבטחה כמו Cure53 לבדיקת האפליקציות והשרתים שלהם. [4]

5. מקורות ברית EYES-5

שותפות המודיעין Five Eyes של ארה"ב, בריטניה, קנדה, אוסטרליה וניו זילנד צמחה משיתוף פעולה של מודיעין אותות בין בעלות הברית בתקופת מלחמת העולם השנייה.

6. בדיקת מנות עמוקה

חומות אש מתקדמות מפעילות בדיקת מנות עמוקה (DPI) כדי לנתח מטא-נתוני מנות רשת ולחסום מאפיינים סטנדרטיים של חיבורי VPN.

7. שימוש ארגוני

ארגונים רבים נותנים לעובדים מרוחקים VPN כדי לגשת למערכות פנימיות כמו מסדי נתונים, ולכן VPN הוא כלי אבטחה נפוץ במקום העבודה.

8. VPN מבוזרים

רשתות VPN מבוזרות (dVPN) מפזרות תעבורה על פני רשת של צמתים המופעלים על ידי עמיתים, ומפחיתות את התלות בספק מרכזי יחיד.

9. אנונימיות ב-Tor לעומת VPN

VPN מנהר את התעבורה דרך ספק יחיד, ואילו Tor (The Onion Router) שולח תעבורה דרך שלושה ממסרים של מתנדבים (שומר, אמצעי, יציאה) כדי למקסם את הפרטיות. [5]

10. עלות הפרצות לנתונים

שילוב של VPN עם מודל גישה של Zero Trust, הבודק כל משתמש וכל מכשיר, עוזר לארגונים להגן על נתונים ולהגביל את הנזק של פרצות נתונים.

מקורות והפניות טכניים

פרסומים מצוטטים, מפרטי הצפנה ותקני מסמכים רשמיים שבהם נעשה שימוש בדף עבודה זה.

מקורות אקדמיים ותעשייתיים

[1] Electronic Frontier Foundation. (2026). Choosing the VPN That's Right for You.
https://ssd.eff.org/module/choosing-vpn-thats-right-you

[2] Federal Trade Commission. (2018). FTC Provides Tips for Using VPN Apps.
https://www.ftc.gov/news-events/news/press-releases/2018/02/ftc-provides-tips-using-vpn-apps

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

[4] Yahoo Finance. (2026). NordVPN passes its no-logs assurance assessment for the sixth time.
https://finance.yahoo.com/news/nordvpn-passes-no-logs-assurance-140000101.html

[5] Tor Project. (n.d.). Overview.
https://support.torproject.org/about-tor/how-tor-works/overview/

מפתח תשובות: הערכת ספקי VPN, תקני אבטחה, ביקורות ומדיניות רישום

1 מדיניות יומנים שנבדקה בביקורת — פרוטוקולים

תשובה נכונה: B

הערה למורה

מדיניות אי-רישום שנבדקה בביקורת עצמאית היא הדרך המעשית ביותר לבדוק טענות פרטיות של אפס ידע של ספק. שיווק מרשים או טענות עצמיות אינם מספיקים. מקור: Deloitte Advisory, Cure53 Audit.

2 עליונות WireGuard — זמן השהיה

תשובה נכונה: D

הערה למורה

WireGuard מציע ניתוב חיבורים מודרני ומהיר במרחב הקרנל עם בסיס קוד קומפקטי (כ-4,000 שורות), מה שהופך ביקורות ליעילות מאוד. מקור: IETF Protocol RFC, WireGuard Project.

3 שאלה 3

תשובה נכונה: B

הערה למורה

VPN חינמיים עדיין משלמים עבור שרתים, וה-FTC מזהיר שחלק מאפליקציות ה-VPN משתפות נתוני משתמשים עם צדדים שלישיים, למשל כדי להציג פרסומות.

4 תחומי שיפוט משפטיים — בקרות ניתוב

תשובה נכונה: C

הערה למורה

השיפוט קובע אם ה-VPN כפוף לחוקי מעקב, לדרישות שמירת נתונים מקומיות ולצווי זימון ממשלתיים חשאיים. מקור: Privacy Rights Clearinghouse.

5 הגנת KILL SWITCH — פרטיות

תשובה נכונה: A

הערה למורה

מתג הקטיעה מנתק מיד את ניתוב מתאם הרשת של המערכת אם המנהרה נופלת, ומונע דליפות חשיפה של ה-IP האמיתי וה-DNS. מקור: IETF Tunnel RFC.

מפתח תשובות: נקודת ביקורת 2 – נכון או לא נכון

6 **מגבלות נוזקות** הסוואת IP

תשובה נכונה: לא נכון

הערה למורה

VPN מספק צינור מוצפן ומאובטח, אך אינו סורק תוכן או קבצים. נדרשת תוכנת אנטי-וירוס כדי לחסום נוזקות. מקור: Deloitte Advisory.

7 **ביקורת עצמאית** מהירויות

תשובה נכונה: נכון

הערה למורה

דוחות ביקורת מאמתים תצורות תוכנת שרתים, עמידה בהגדרת RAM בלבד והיעדר מסדי נתונים של רישום. ציטוט: Deloitte Advisory, Cure53 Audit.

8 **שאלה 8**

תשובה נכונה: לא נכון

הערה למורה

ספקים חייבים לציית לחוקי מדינת הבית שלהם, שעשויים לכלול כללי שמירת נתונים וצווים למסירת נתונים שבידיהם.

9 **גודל בסיס הקוד של הפרוטוקול** חומות אש

תשובה נכונה: נכון

הערה למורה

בסיס קוד קטן יותר מצמצם את שטח התקיפה האפשרי ומקל על צוותי אבטחה לאמת את שלמות הפרוטוקול. מקור: WireGuard Project.

10 **מונטיזציה של פרסומות** ללא יומנים

תשובה נכונה: נכון

הערה למורה

בהיעדר דמי מנוי, VPN חינמיים מסתמכים על כריית נתונים, יצירת פרופילי תעבורה והזרקת פרסומות לדפדפן כדי ליצור הכנסות. מקור: EDRi Retention Guidelines.

מפתחות אוצר מילים ומחוון הערכה

מחוון הערכה למורה: תנו 1 נקודה לכל התאמה נכונה (סה"כ 8 נקודות) ולכל מונח הקשר (סה"כ 6 נקודות).

נקודת ביקורת 4: מפתח תשובות – התאמת מושגים

F 1. WireGuard	H 2. יומנים מבוקרים	E 3. שיפוט	B 4. מתג חירום (Kill Switch)
C 5. Five Eyes	A 6. VPN חינמי	D 7. שרתי RAM בלבד	G 8. OpenVPN

נקודת ביקורת 3: מפתח תשובות – מונחי מפתח

1 אפס יומנים	2 וויירגארד	3 מתג הפסקה	4 סמכות שיפוט
5 זיכרון בלבד	6 ביקורת		

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

1 E – חמשעיניים	2 A – וויירגארד	3 H – קודפתוח	4 F – חינמי
5 D – מתגהפסקה	6 G – זיכרוןבלבד	7 C – סמכותשיפוט	8 B – אפסיומנים

הערות לדיון עבור מורים

מונחי מפתח:
ודאו שהתלמידים מסבירים במילים שלהם את WireGuard, יומנים מבוקרים ו-שיפוט ונותנים דוגמה לכל אחד מהם.

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

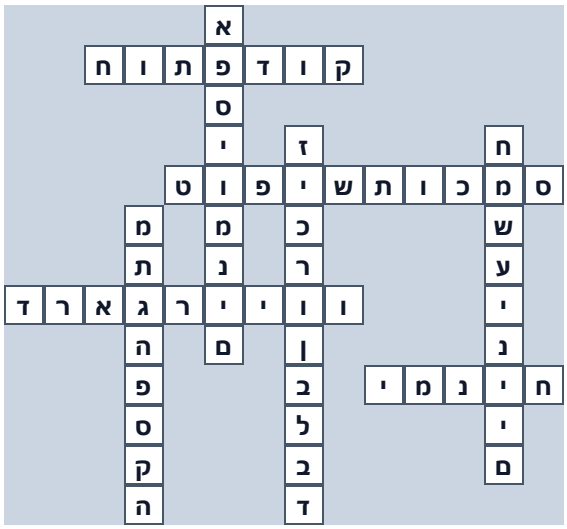
הערכת מקורות:
בקשו מהתלמידים לאמת לפחות טענה אחת במקורות של דף העבודה, ודונו מדוע נתונים, מחירים וכללים עשויים להשתנות עם הזמן.

מפתחות פאזלים והערות למורה

פתרון תפזורת

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

פתרון תשבץ



מדריך למורה לפתרונות התשבץ

מאוזן

2 מאוזן: קודפתוח פרוטוקול בוגר ומבוקר רבות, עם בסיס קוד גדול בהרבה מזה של WireGuard (7 אותיות)

5 מאוזן: סמכותשיפוט האזור הגאוגרפי השולט בהתחייבויות המשפטיות של ספק ה-VPN (10 אותיות)

7 מאוזן: וויירגארד פרוטוקול מודרני ומהיר המבוסס על כ-4,000 שורות קוד הניתנות לביקורת בקלות (9 אותיות)

8 מאוזן: חינמי שירות חיבור בסיכון גבוה שלעתים מרוויח מתיעוד ומכירה של נתוני גלישה (5 אותיות)

מאונך

1 מאונך: אפסיומנים טענת פרטיות שאומתה על ידי חברות אבטחת סייבר עצמאיות של צד שלישי (9 אותיות)

3 מאונך: חמשעיניים ברית שיתוף מודיעין בינלאומית בין ארה״ב, בריטניה, קנדה, אוסטרליה וניו זילנד (9 אותיות)

4 מאונך: זיכרונבלבד תשתית חומרה הפועלת כולה על זיכרון נדיף ומונעת אחסון נתונים (10 אותיות)

6 מאונך: מתגהפסקה מנגנון בטיחות החוסם ניתוב אינטרנט אם המנהרה המאובטחת מתנתקת (8 אותיות)

מפתח פתרונות: מילים מבולבלות ופענוח הצופן

מפתח הערכה לפעילות פענוח מילות אוצר המילים ולאתגר הצופן הסודי.

מפתח פענוח מילים מבולבלות

1. גריווארדי — וויירגארד
2. ווסמתטיפשכ — סמכותשיפוט
3. חנימיסעיש — חמשעיניים
4. ן‌בודרלבזיכ — זיכרון‌בלבד
5. נופסמיאיס — אפסיומנים
6. קההסמפתג — מתגהפסקה
7. מיחני — חינמי
8. ופחקותד — קודפתוח

מפתח אתגר הצופן הסודי

"השוו דוחות עם מערכת מאובטחת"

מפתח תשובות למקרי הבוחן

A תרחיש A: אבטחת רשת ציבורית

האזנה והצפנה | הדילמה של שרה

הנחיות הערכה

תשובות התלמידים צריכות לכלול את הנקודות הבאות:

- סיכונים: האזנה לחבילות, יירוט נתונים והתקפות אדם בתווך (man-in-the-middle). מישהו באותה רשת של בית הקפה יכול ללכוד את פרטי ההתחברות שלה או את קובץ שיעורי הבית.
- הגנת VPN: מצפין את מטעני מנות הרשת, ובכך הופך תעבורת מנהרה שיורטה לבלתי קריאה למאזינים פסיביים ברשת המקומית כאשר ה-VPN מוגדר נכון.

B תרחיש B: גישה למשאבים חסומים

חסימה גאוגרפית וכתובות IP | הדילמה של אלכס

הנחיות הערכה

תשובות התלמידים צריכות לכלול את הנקודות הבאות:

- סיבת החסימה: מארח הסטרימינג משתמש בחסימה גיאוגרפית, הממפה את כתובת ה-IP המקומית של הנוסע למדינה הפיזית שלו וחוסמת אותה על סמך רישוי טריטוריאלי.
- כיצד VPN עוזר: הסתרת מיקומו האמיתי על ידי ניתוב התעבורה דרך שרת במדינת הבית שלו. האתר רואה את כתובת ה-IP של מדינת הבית, ולכן מתאפשרת הגישה.