שם: _____ תאריך: _____ ציון: _____

מדריך VPN של VPN.com
דף עבודה

תרגילים מעשיים בפרוטוקולי רשת, מנהור ובקרות אבטחה.

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

- הסבירו את המושג מנהור נתונים ועטיפה.
- זהו תצורות פרוטוקול סטנדרטיות ודרישות רוחב פס.
- נתחו את תפקידם של חומות אש וחסימות גיאוגרפיות בניתוב באינטרנט.
- הבינו כיצד ספקי אינטרנט עוקבים אחר גלישה לא מוצפנת וכיצד VPN מונע זאת.
- הבחינו בין גבולות התפעול של מיקום השרת לבין השיפוט.

הוראות מדריך VPN

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 תרחישים אמיתיים בחלק מקרי הבוחן. ולסיום, פעילות הבונוס "חשבו מהר".

מהו VPN? (מבוא)

רשת וירטואלית פרטית היא יותר מסתם מתג פרטיות. זוהי מנהרה מוצפנת שמנתבת את תעבורת האינטרנט שלך דרך שרת מרוחק. היא מסתירה את כתובת ה-IP שלך, מונעת מספק האינטרנט שלך לאסוף יומנים של פעולותיך המקוונות, ומאבטחת את הנתונים שלך ברשתות ציבוריות. הבנת המונחים חיונית לשמירה על בטיחות דיגיטלית.

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

נקודת ביקורת 1: אתגר שאלות אמריקאיות

1. מהו פרוטוקול VPN?

- A. התקן חומרה שמשמש לחיבור כבלים.
- B. סט כללים המגדיר כיצד נתונים מוצפנים ונשלחים.
- C. תוסף דפדפן החוסם פרסומות.
- D. חברת ספק שירותי אינטרנט.

2. אם חיבור ה-VPN שלכם מרגיש איטי, מהי הסיבה הסבירה ביותר?

- A. שרת ה-VPN רחוק מדי או עמוס מדי.
- B. רזולוציית המסך שלכם מוגדרת גבוהה מדי.
- C. השבתתם את העוגיות בדפדפן.
- D. פריסת המקלדת שלכם מוגדרת באופן שגוי.

3. מדוע VPN מומלץ מאוד בעת חיבור לרשת Wi-Fi ציבורית?

- A. הוא הופך את חיבור ה-Wi-Fi לחינמי.
- B. הוא מגדיל את טווח הנתב.
- C. הוא מצפין תעבורה כדי לחסום האקרים באותה רשת.
- D. הוא מוחק דואר זבל אוטומטית.

4. איזו מהאפשרויות הבאות מתארת חסימה גיאוגרפית (geoblock)?

- A. כלי שמודד מרחק פיזי לשרת.
- B. הגבלה החוסמת גישה לאתר לפי מיקום.
- C. פרוטוקול לדחיסת קבצים מקומיים.
- D. מנגנון אחסון גיבוי.

5. מה ספק שירותי האינטרנט (ISP) שלכם יכול לראות כשאתם משתמשים ב-VPN?

- A. מילות מפתח לחיפוש ותוכן דפי אינטרנט שאתה צופה בהם.
- B. שאתם מחוברים ל-VPN, אך לא פרטי התעבורה.
- C. שום מידע, אפילו לא על כך שאתם מחוברים לרשת.
- D. הקבצים והתמונות שלכם בכונן הקשיח המקומי.

נקודת ביקורת 2: אתגר נכון או לא נכון

6 הסתרת מיקום

6. VPN מסתיר את כתובת ה-IP הציבורית של המכשיר שלך ומקשה על אתרי צד שלישי לזהות בקלות את מיקומך הפיזי.

נכון לא נכון

7 השפעת VPN על המהירות

7. הפעלת חיבור VPN הופכת את מהירות האינטרנט הבסיסית שלכם למהירה פי שניים מחיבור ללא VPN.

נכון לא נכון

8 ציתות ב-Wi-Fi ציבורי

8. אם אתם משתמשים ברשת Wi-Fi ציבורית לא מאובטחת בלי VPN, משתמשים אחרים באותה רשת עלולים ללכוד את התעבורה הלא מוצפנת שלכם.

נכון לא נכון

9 חומות אש וחיבורים חסומים

9. מנהלי רשת יכולים להגדיר חומות אש כך שיזהו ויחסמו מנהרות VPN יוצאות.

נכון לא נכון

10 מדיניות קפדנית של אפס יומנים

10. מדיניות "אפס יומנים" קפדנית פירושה שספק ה-VPN מחויב על פי חוק לאחסן את שאילתות החיפוש ואת הקישורים שבהם ביקרת למשך 30 ימים לפחות.

נכון לא נכון

נקודת ביקורת 3: השלמת מונחי מפתח

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

1. כדי לאבטח את התעבורה שלכם, ה-VPN עוטף את מנות הנתונים בתוך פרוטוקול אחר, תהליך המכונה _____ .
2. אם אתם חווים מהירויות הורדה איטיות בסטרימינג, ייתכן שהסיבה היא _____ מוגבל ברשת.
3. שירות סטרימינג הזמין רק במדינה מסוימת מגביל משתמשים בעולם באמצעות _____ גיאוגרפית.
4. כללי החיבור המגדירים את פרמטרי ההצפנה והחיבור נקראים _____ ה-VPN.
5. המחשב שלכם מסתמך על _____ מקומית כדי לנטר תעבורת רשת ולחסום חיבורים לא בטוחים.
6. כשאתם מתחברים ל-VPN, הנתונים שלכם מנותבים דרך _____ מרוחק כדי להסתיר את כתובת ה-IP הציבורית שלכם.

בנק מילים

חומת אש | חסימה | מנהור | ספק אינטרנט | פרוטוקול | פרטיות | רוחב פס | שרת

כתבו את תשובותיכם כאן:

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

נקודת ביקורת 4: התאמת מושגים ברשתות

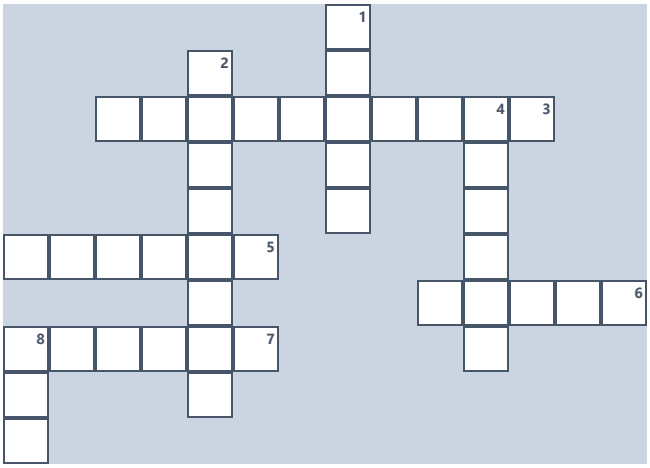
התאמת הגדרות

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

1. מנהור	A	קבוצת כללים שקובעת כיצד נתונים מועברים ברשת.
2. פרוטוקול	B	הקצב המרבי של העברת נתונים לאורך חיבור.
3. רוחב פס	C	הגבלה שמונעת גישה לאינטרנט על בסיס מיקום פיזי.
4. שרת	D	מערכת אבטחה שמנטרת וחוסמת תעבורה לא מורשית.
5. חסימה גיאוגרפית	E	מחשב מרוחק שמנתב את התעבורה שלך ומסתיר את כתובת ה-IP שלך.
6. חומת אש	F	מצב של היעדר מעקב או מעקב ציבורי.
7. פרטיות	G	ספק שירותי אינטרנט שנושא את התעבורה שלכם ויכול לראות פעילות לא מוצפנת.
8. ספק אינטרנט (ISP)	H	עטיפת חבילות נתונים בתוך חבילה אחרת להעברה מאובטחת.

נקודת ביקורת 5: תשבץ

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



מאונך

1. הגבלה המונעת גישה לאתרים לפי מיקום פיזי (5)
2. קבוצת כללים הקובעת כיצד נתונים מועברים ברשת (8)
4. מצב של היעדר מעקב או מעקב ציבורי (6)
8. מחשב מרוחק המנתב את התעבורה שלך ומסתיר את כתובת ה-IP שלך (3)

מאוזן

3. חברה המספקת גישה לאינטרנט ורושמת את התעבורה שלך אלא אם היא מוצפנת (10)
5. קצב העברת הנתונים המרבי לאורך חיבור (6)
6. עטיפת מנות נתונים בתוך מנה אחרת למעבר מאובטח (5)
7. מערכת אבטחה המנטרת וחוסמת תעבורה לא מורשית (6)

נקודת ביקורת 5 – פעילות חלופית: רמזים נגישים לתשבץ

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

מאוזן

3 מאוזן: חברה המספקת גישה לאינטרנט ורושמת את התעבורה שלך אלא אם היא מוצפנת (10 אותיות):

5 מאוזן: קצב העברת הנתונים המרבי לאורך חיבור (6 אותיות):

6 מאוזן: עטיפת מנות נתונים בתוך מנה אחרת למעבר מאובטח (5 אותיות):

7 מאוזן: מערכת אבטחה המנטרת וחוסמת תעבורה לא מורשית (6 אותיות):

מאונך

1 מאונך: הגבלה המונעת גישה לאתרים לפי מיקום פיזי (5 אותיות):

2 מאונך: קבוצת כללים הקובעת כיצד נתונים מועברים ברשת (8 אותיות):

4 מאונך: מצב של היעדר מעקב או מעקב ציבורי (6 אותיות):

8 מאונך: מחשב מרוחק המנתב את התעבורה שלך ומסתיר את כתובת ה-IP שלך (3 אותיות):

נקודת ביקורת 6: חיפוש מילה נסתרת

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

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

רשימת מילים

מנהור | פרוטוקול | רוחבפס | שרת | חסימה | חומתאש | פרטיות | ספקאינטרנט

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. מנהור
B. פרוטוקול
C. רוחבפס
D. שרת
E. חסימה
F. חומתאש
G. פרטיות
H. ספקאינטרנט

הגדרות ושדות התאמה	
1. מצב של היעדר מעקב או מעקב ציבורי.	
2. הגבלה המונעת גישה לאתרים לפי מיקום פיזי.	
3. קבוצת כללים הקובעת כיצד נתונים מועברים ברשת.	
4. מערכת אבטחה המנטרת וחוסמת תעבורה לא מורשית.	
5. קצב העברת הנתונים המרבי לאורך חיבור.	
6. מחשב מרוחק המנתב את התעבורה שלך ומסתיר את כתובת ה-IP שלך.	
7. חברה המספקת גישה לאינטרנט ורושמת את התעבורה שלך אלא אם היא מוצפנת.	
8. עטיפת מנות נתונים בתוך מנה אחרת למעבר מאובטח.	

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. והמרנ
2. סרחפבו
3. יחהמס
4. תיטופר
5. וקרלטפוו
6. רתש
7. אחתשמו
8. נאנטסיפטרק

פעילות בונוס: חשבו מהר

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

1	דברים שאתם מקשרים למילה "מנהרה"		
2	דברים שהייתם מלמדים את המשפחה שלכם על VPN		
3	דברים באתר שיכולים לעקוב אחריכם		
4	מיתוסים על VPN		
5	מילים מדף העבודה הזה שתרצו לזכור		
6	מכשירים שיכולים להשתמש ב-VPN		
7	דברים ש-VPN לא יכול להגן עליכם מפניהם		
8	מדינות שהייתם רוצים "לבקר" בהן באינטרנט		
9	הבטחות שספק VPN טוב מבטיח		
10	דרכים לזהות רשת Wi-Fi מזויפת		
11	שאלות שיש לכם על VPN		
12	שירותי VPN שאתם מכירים		
13	מילים הקשורות לפרטיות		
14	דברים ש-VPN יכול להסתיר		
15	סיבות להשתמש ב-VPN בבית קפה		

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

VPN מצפין את התעבורה שלך כדי לאבטח אותה. השתמשו במפתח האותיות-למספרים שלהלן כדי לפענח את ההודעה בנושא אבטחת סייבר, 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

22	20	7	16	2		22	6	10	9	20	17	5		12	16		6	14	3	5

22	8	9	2	6	1	13		5	20	5	14	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: האם חוקי להשתמש ב-VPN?

השימוש ב-VPN חוקי במדינות רבות, אך בחלק מסמכויות השיפוט מגבילים, מסדירים או חוסמים שירותי VPN. על המשתמשים לוודא את החוקים המקומיים העדכניים לפני השימוש. לפרטים נוספים, עיינו במדריכי החוקיות ב-VPN.com.

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-iOS, Android, macOS, Windows, Linux 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. [3]

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 תעבורת ה-VPN כך שתיראה כתעבורת HTTPS רגילה (פורט 443). הדבר יכול לסייע 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 Eyes 5/9/14 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: האם VPN יכול לעקוף האטת אינטרנט מצד ספק האינטרנט?

לפעמים. VPN עשוי לעזור כאשר ספק אינטרנט מאט באופן סלקטיבי פעילויות הניתנות לזיהוי, אך הוא לא יתגבר על עומס, מכסות נתונים, מגבלות מהירות ברמת החשבון או איכות רשת ירודה.

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) פותח על ידי קבוצת ספקים שכללה את Microsoft ופורסם כ-RFC 2637 ביולי 1999 כדי לתמוך ב-VPN לגישה מרחוק. [6]

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 מבקרים חיצוניים (כמו Cure53 או PwC) לביצוע סקירות קוד עצמאיות ולאימות שהם אינם רושמים פעילות משתמשים.

5. מקורות ברית EYES-5

ברית Five Eyes צמחה מהסכם מודיעין האותות UKUSA משנת 1946 בין ארה"ב לבריטניה, שאליו הצטרפו מאוחר יותר קנדה, אוסטרליה וניו זילנד.

6. בדיקת מנות עמוקה

בדיקת חבילות עמוקה (DPI) בוחנת את תוכן החבילות ואת דפוסי התעבורה, ולא רק את הכותרות, וחלק מחומות האש משתמשות בה כדי לזהות ולחסום פרוטוקולי VPN נפוצים.

7. שימוש ארגוני

אחוז גדול מעובדי ארגונים ברחבי העולם משתמשים ב-VPN מאובטחים כדי להתחבר למסדי נתונים פנימיים, מה שהופך אותו לתקן אבטחה מרכזי.

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 ויציאה), כך שאף ממסר יחיד אינו מכיר את שני הקצוות.

10. עלות הפרצות לנתונים

אימוץ מודל גישה מאובטחת של אפס אמון עם VPN עוזר לארגונים להגן על קניין רוחני ולצמצם את ההשפעה הכספית של דליפות נתונים.

מקורות והפניות טכניים

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

ספרות אקדמית ותקני אבטחה

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

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

סיכום תקנים טכניים

- תקני עטיפה: RFC 4301 מגדיר ניתוב מאובטח של חבילות אינטרנט ב-IPsec/L2TP.
- מעקב של ספק האינטרנט: ניתוב שאילתות DNS דרך מנהרת ה-VPN המוצפנת יכול לצמצם את חשיפת ה-DNS לספק האינטרנט המקומי.
- פרוטוקולי בקרת חומת אש: חבילות Stealth מוסוות עוקפות מסנני חבילות עמוקים.

מפתח תשובות: נקודת ביקורת 1 – שאלות אמריקאיות

1 שאלה 1

תשובה נכונה: B

הערה למורה

פרוטוקול VPN מגדיר את הכללים לבניית המנהרה ולהצפנת הנתונים; האפשרויות האחרות מתארות כבלים, חוסמי פרסומות וספקי אינטרנט.

2 שאלה 2

תשובה נכונה: A

הערה למורה

מרחק מוסיף השהיה ושרת עמוס מדי יש לו פחות קיבולת לחלוק; רזולוציית מסך, עוגיות ופריסת מקלדת אינן משפיעות על מהירות החיבור.

3 שאלה 3

תשובה נכונה: C

הערה למורה

ברשתות פתוחות אחרים יכולים ליירט מנות לא מוצפנות; VPN מצפין את התעבורה כך שנתונים שיורטו אינם ניתנים לקריאה.

4 שאלה 4

תשובה נכונה: B

הערה למורה

חסימה גיאוגרפית מתאימה את כתובת ה-IP הציבורית של מבקר למאגר מיקומים ושוללת גישה מחוץ לטריטוריות המותרות.

5 שאלה 5

תשובה נכונה: B

הערה למורה

ספק האינטרנט יכול לראות שאתם שולחים נתונים מוצפנים לשרת VPN, אך לא באילו אתרים אתם מבקרים או מה אתם מחפשים.

מפתח תשובות: נקודת ביקורת 2 – נכון או לא נכון

6 שאלה 6

תשובה נכונה: נכון

הערה למורה

אתרים רואים את כתובת ה-IP של שרת ה-VPN במקום שלכם, מה שמסתיר מהם את המיקום המשוער שלכם.

7 שאלה 7

תשובה נכונה: לא נכון

הערה למורה

הצפנה והדילוג הנוסף לשרת ה-VPN מפחיתים בדרך כלל מעט את המהירות; VPN אינו יכול להכפיל את מהירות החיבור הבסיסית שלכם.

8 שאלה 8

תשובה נכונה: נכון

הערה למורה

ב-Wi-Fi לא מאובטח, כלי האזנה למנות יכולים ללכוד תעבורה לא מוצפנת כמו התחברויות שנשלחות בלי HTTPS.

9 שאלה 9

תשובה נכונה: נכון

הערה למורה

מנהלים יכולים לחסום יציאות VPN מוכרות, כמו 1194 של OpenVPN, או להשתמש ב-Deep Packet Inspection כדי לזהות תעבורת VPN.

10 שאלה 10

תשובה נכונה: לא נכון

הערה למורה

מדיניות אי-שמירת יומנים היא הבטחה של ספק לא לשמור רשומות של הפעילות שלכם; אין חוק שמחייב VPN לאחסן חיפושים למשך 30 ימים.

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

H 1. מנהור	A 2. פרוטוקול	B 3. רוחב פס	E 4. שרת
C 5. חסימה גיאוגרפית	D 6. חומת אש	F 7. פרטיות	G 8. ספק אינטרנט (ISP)

נקודת ביקורת 3: מפתח תשובות – מונחי מפתח

1 מנהור	2 רוחב פס	3 חסימה	4 פרוטוקול
5 חומת אש	6 שרת		

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

1 G – פרטיות	2 E – חסימה	3 B – פרוטוקול	4 F – חומתאש
5 C – רוחבפס	6 D – שרת	7 H – ספקאינטרנט	8 A – מנהור

הערות לדיון עבור מורים

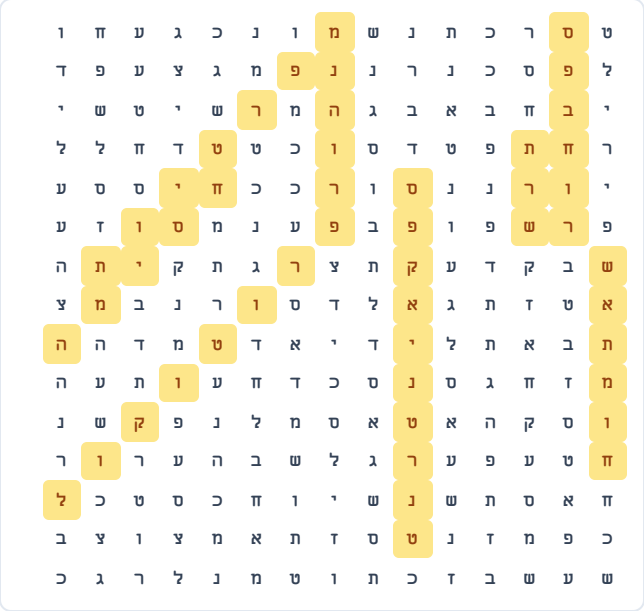
מונחי מפתח:
ודאו שהתלמידים מסבירים במילים שלהם את מנהור, פרוטוקול ו-רוחב פס ונותנים דוגמה לכל אחד מהם.

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

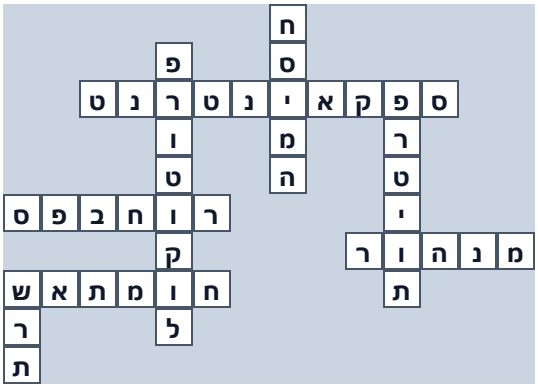
הערכת מקורות:
בקשו מהתלמידים לאמת לפחות טענה אחת במקורות של דף העבודה, ודונו מדוע נתונים, מחירים וכללים עשויים להשתנות עם הזמן.

מפתחות פאזלים והערות למורה

פתרון תפזורת



פתרון תשבץ



מאוזן

3 מאוזן: ספקאינטרנט חברה המספקת גישה לאינטרנט ורושמת את התעבורה שלך אלא אם היא מוצפנת (10 אותיות)

5 מאוזן: רוחבפס קצב העברת הנתונים המרבי לאורך חיבור (6 אותיות)

6 מאוזן: מנהור עטיפת מנות נתונים בתוך מנה אחרת למעבר מאובטח (5 אותיות)

7 מאוזן: חומתאש מערכת אבטחה המנטרת וחוסמת תעבורה לא מורשית (6 אותיות)

מאונך

1 מאונך: חסימה הגבלה המונעת גישה לאתרים לפי מיקום פיזי (5 אותיות)

2 מאונך: פרוטוקול קבוצת כללים הקובעת כיצד נתונים מועברים ברשת (8 אותיות)

4 מאונך: פרטיות מצב של היעדר מעקב או מעקב ציבורי (6 אותיות)

8 מאונך: שרת מחשב מרוחק המנתב את התעבורה שלך ומסתיר את כתובת ה-IP שלך (3 אותיות)

מפתח פתרונות: מילים מבולבלות ופענוח הצופן

מפתח הערכה לפעילות פענוח מילות אוצר המילים ולאתגר הצופן הסודי.

מפתח פענוח מילים מבולבלות

1. והמרנ — מנהור
2. סרחפבו — רוחבפס
3. יחהמס — חסימה
4. תיטופר — פרטיות
5. וקרלטפוו — פרוטוקול
6. רתש — שרת
7. אחתשמו — חומתאש
8. נאנטסיפטרק — ספקאינטרנט

מפתח אתגר הצופן הסודי

"הגנו על הפרטיות בעזרת מנהרה 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.