שם: _____ תאריך: _____ ציון: _____

מדריך ה-VPN המאובטח ביותר

ניתוח טכני של עיצוב VPN בעל אבטחה גבוהה, שרתי זיכרון נדיף מבוססי RAM בלבד, אבטחת גישה מסוג Zero Trust, הגנות פרטיות מוצפנות מפני דליפות DNS ותצורות WireGuard שנבדקו בביקורת.

סקירת למידה: ה-VPN המאובטח ביותר

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 התקנים הטכניים של VPN מאובטחים במיוחד. תחקרו חומרת שרתים מסוג RAM בלבד, אבטחת גישה של Zero Trust, פותרי DNS פרטיים ומוצפנים והגדרות WireGuard מבוקרות.

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/most-secure-vpn/

מפת הלמידה שלכם: ה-VPN המאובטח ביותר

- נתחו את הארכיטקטורה הטכנית ותקני ההצפנה של המדריך ל-Most Secure VPN.
- הגדירו את הגדרות הלקוח כדי למנוע דליפות תעבורה של IP, DNS ו-WebRTC.
- השוו פרוטוקולי מנהור קנייניים להטמעות רגילות.

הוראות למדריך ה-VPN המאובטח ביותר

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 חומרת שרתים מבוססת RAM בלבד ומערכות Zero Trust. ולסיום, פעילות הבונוס "חשבו מהר".

תשתיות RAM בלבד ורשתות Zero Trust (מבוא)

VPN מאובטח באמת מסתמך על מסגרת zero trust, שרתי RAM בלבד כדי למנוע חשיפת יומנים בעקבות תפיסת דיסקים, פותרי DNS פרטיים ומוצפנים ופרוטוקולים שנבדקו כמו WireGuard. בקרות משולבות אלה מגינות על נכסים דיגיטליים בעלי ערך גבוה מפני איומי יירוט.

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

נקודת ביקורת 1: אתגר שאלות אמריקאיות

1 1. איזו ארכיטקטורה היא בסיסית להבטחת רמת האבטחה הגבוהה ביותר בשרתי VPN מודרניים?

- A) תשתית שרתי RAM בלבד
- B) אחסון מבוסס דיסק
- C) ניתוב Dynamic DNS
- D) הפעלת העברת יציאות

2 2. איזה פרוטוקול מומלץ באופן נרחב לתצורות VPN המאובטחות והמודרניות ביותר?

- A) WireGuard
- B) PPTP
- C) L2TP/IPSec
- D) SSTP

3 3. איזו מסגרת אבטחה מחייבת אימות רציף של כל חיבור ללא יוצא מן הכלל?

- A) ארכיטקטורת Zero Trust
- B) חומות אש היקפיות
- C) ניתוב דינמי
- D) מפתחות סודיים משותפים

4 4. מהו התפקיד העיקרי של הגנת דליפות DNS בלקוח VPN?

- A) ניתוב כל בקשות ה-DNS דרך פותרים פרטיים ומוצפנים
- B) טשטוש חבילות IP
- C) שמירת שאילתות DNS במטמון מקומי
- D) השבתת שרתי שמות

5 5. כיצד ניתוב Multi-Hop מגביר את האבטחה הכוללת של מנהרת VPN?

- A) מנתב נתונים דרך שני שרתים נפרדים ברצף
- B) מגביר את מהירות הדחיסה
- C) מצפין נתונים בצפנים בעלי אבטחה נמוכה
- D) עוקף חומות אש

נקודת ביקורת 2: אתגר נכון או לא נכון

6 שאלה 6

6. שרתי RAM בלבד שומרים קובצי יומן בזיכרון זמני, שנמחק באתחול מחדש.

נכון לא נכון

7 שאלה 7

7. WireGuard משתמש באלגוריתמים קריפטוגרפיים מודרניים שפחות חשופים לצווארי בקבוק של מהירות.

נכון לא נכון

8 שאלה 8

8. מתג חירום של VPN פועל על ידי חסימת כל תעבורת הרשת אם המנהרה נופלת.

נכון לא נכון

9 שאלה 9

9. ביקורות עצמאיות של צד שלישי אינן רלוונטיות לאימות התחייבויות אבטחה.

נכון לא נכון

10 שאלה 10

10. מודלים של Zero Trust מניחים שכל חיבורי הרשת הפנימיים מאובטחים כברירת מחדל.

נכון לא נכון

נקודת ביקורת 3: השלמת מונחי מפתח

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

1. מנהלי מערכת אוכפים אבטחה על ידי פריסת מסגרת _____ קפדנית.
2. ניתוב מנות דרך כמה נקודות כניסה מחייב תצורה מאובטחת של _____ .
3. כדי למנוע דליפות נתונים מכוננים גנובים, אנו משתמשים בתכנון של שרת _____ .
4. חטיפת ספק האינטרנט מנוטרלת באמצעות הגדרת תכונות מובנות של _____ .
5. כדי לחסום תעבורה בזמן כשלי חיבור, הפעילו את המנגנון הנקרא _____ .
6. כדי למזער יומנים השמורים במסד נתונים, בחרו ספק _____ לחלוטין.

בנק מילים

אפס אמון | הגנת DNS | הצפנה | זיכרון בלבד פרוטוקול | מבוקר | מתג הפסקה | ניתוב כפול

כתבו את תשובותיכם כאן:

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

נקודת ביקורת 4: התאמת מושגים ב-VPN וברשתות

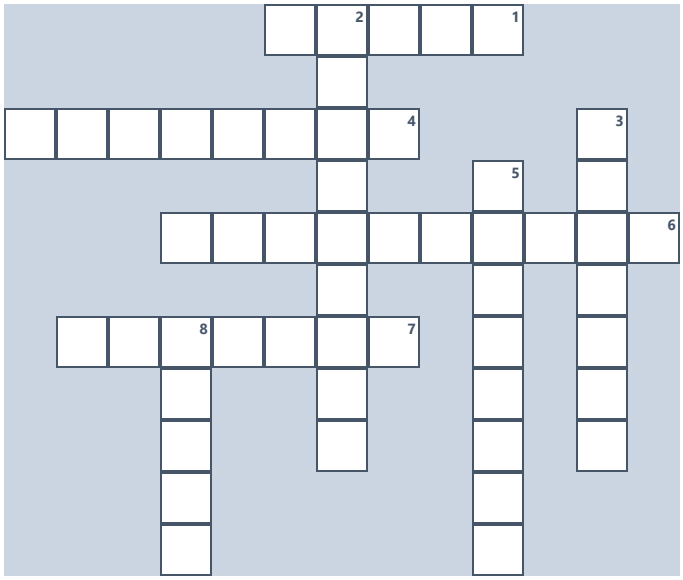
התאמת הגדרות

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

1. Zero Trust	A	מערך שנבדק באופן עצמאי ומאשר שלא נשמרים יומנים.
2. Multi-Hop	B	ערבול קריפטוגרפי של מטען נתונים לאבטחת המעבר.
3. שרת RAM בלבד	C	מסגרת אבטחה הדורשת אימות רציף של כל המשתמשים.
4. הגנת DNS	D	קבוצת כללים טכניים הקובעים כיצד נתונים נארזים ונשלחים.
5. KILL SWITCH	E	ניתוב VPN מדורג המחבר שני צמתי שרת בשרשרת.
6. מערכת שנבדקה בביקורת	F	ארכיטקטורת שרת המשתמשת בזיכרון נדיף לאחסון מטעני נתונים.
7. הצפנה	G	אכיפת שאילתות DNS פרטיות כדי להגן על חיפושי שרתי שמות.
8. פרוטוקול	H	מנגנון כשל בטוח החוסם תעבורה אם ה-VPN נכשל.

נקודת ביקורת 5: תשבץ

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



מאוזן

1. ערבול קריפטוגרפי של מטעני נתונים לאבטחת המעבר (5)

4. מנגנון הגנה החוסם תעבורה אם ה-VPN נכשל (8)

6. ארכיטקטורת שרתים המשתמשת בזיכרון נדיף לאחסון מטעני נתונים (10)

7. מסגרת אבטחה הדורשת אימות מתמשך של כל המשתמשים (7)

מאונך

2. ניתוב VPN במפל המשרשר שני צמתי שרת (9)

3. אכיפת בקשות DNS פרטיות להגנה על חיפושי שרתי השמות (7)

5. קבוצת כללים טכניים הקובעים כיצד נתונים נארזים ונשלחים (8)

8. מערך שנבדק באופן עצמאי ומאשר שלא נשמרים יומנים (5)

נקודת ביקורת 5 – פעילות חלופית: רמזים נגישים לתשבץ

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

מאוזן

1 מאוזן: ערבול קריפטוגרפי של מטעני נתונים לאבטחת המעבר (5 אותיות):

4 מאוזן: מנגנון הגנה החוסם תעבורה אם ה-VPN נכשל (8 אותיות):

6 מאוזן: ארכיטקטורת שרתים המשתמשת בזיכרון נדיף לאחסון מטעני נתונים (10 אותיות):

7 מאוזן: מסגרת אבטחה הדורשת אימות מתמשך של כל המשתמשים (7 אותיות):

מאונך

2 מאונך: ניתוב VPN במפל המשרשר שני צמתי שרת (9 אותיות):

3 מאונך: אכיפת בקשות DNS פרטיות להגנה על חיפושי שרתי השמות (7 אותיות):

5 מאונך: קבוצת כללים טכניים הקובעים כיצד נתונים נארזים ונשלחים (8 אותיות):

8 מאונך: מערך שנבדק באופן עצמאי ומאשר שלא נשמרים יומנים (5 אותיות):

נקודת ביקורת 6: חיפוש מילה נסתרת

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

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

רשימת מילים

אפסאמון | ניתובכפול | זיכרוןבלבד | שאילתות פרוטוקול | מתגהפסקה | מבוקר | הצפנה

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. אפסאמון
B. ניתובכפול
C. זיכרונבלבד
D. שאילתות
E. מתגהפסקה
F. מבוקר
G. הצפנה
H. פרוטוקול

	הגדרות ושדות התאמה
	1. מנגנון הגנה החוסם תעבורה אם ה-VPN נכשל.
	2. אכיפת בקשות DNS פרטיות להגנה על חיפושי שרתי השמות.
	3. ניתוב VPN במפל המשרשר שני צמתי שרת.
	4. קבוצת כללים טכניים הקובעים כיצד נתונים נארזים ונשלחים.
	5. ערבול קריפטוגרפי של מטעני נתונים לאבטחת המעבר.
	6. ארכיטקטורת שרתים המשתמשת בזיכרון נדיף לאחסון מטעני נתונים.
	7. מערך שנבדק באופן עצמאי ומאשר שלא נשמרים יומנים.
	8. מסגרת אבטחה הדורשת אימות מתמשך של כל המשתמשים.

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. אואמנספ
2. ברזיודבלנכ
3. התמפסהקג
4. פהנהצ
5. פביל כונות
6. ויתשלתא
7. קרמוב
8. טרולפוקו

פעילות בונוס: חשבו מהר

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

1	מנעולים או מפתחות שאתם משתמשים בהם כל יום		
2	דברים ש-VPN יכול להסתיר		
3	דברים שהופכים VPN למאובטח		
4	מיתוסים על VPN		
5	סיבות להשתמש ב-VPN בזמן נסיעות		
6	מקומות בטוחים בעולם האמיתי		
7	מילים שפירושן "מוגן"		
8	הבטחות שספק VPN טוב מבטיח		
9	מילים הקשורות לפרטיות		
10	סוגי ביקורת או בדיקה		
11	מילים מדף העבודה הזה שתרצו לזכור		
12	דברים שהאקר רוצה לגנוב		
13	דרכים לזהות רשת Wi-Fi מזויפת		
14	מקומות שבהם תשתמשו ב-VPN		
15	דברים שספק האינטרנט שלכם יכול לראות		

נקודת ביקורת 8: מקרי בוחן ב-VPN וברשתות

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

מקרה בוחן 1: חיזוק תשתית ארגונית



תרחיש: בנק ארגוני מתכנן מחדש את טופולוגיית הגישה מרחוק שלו. הוא דורש ארכיטקטורת Zero Trust שמקשרת את כל מכשירי הלקוח לשרתים מאובטחים.

שאלה לדיון: מהו היתרון העיקרי של מיקרו-סגמנטציה של הרשת במודל VPN מסוג Zero Trust?

מקרה בוחן 2: הגנות של שרתי RAM-Only



תרחיש: ספק VPN ממוקד אבטחה משדרג את השרתים שלו כדי למנוע שתפיסה פיזית של שרת תחשוף היסטוריות יומנים של משתמשים.

שאלה לדיון: הסבירו כיצד תצורות חומרה מסוג RAM-Only מונעות חילוץ נתונים פורנזי בעת תפיסה פיזית של 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

12	16		5	14	10	3	13		5	19	7	8		5	8	9	2	1

24	10	20	19	10		24	10	15	11	14

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: מה הופך VPN ל'מאובטח ביותר'?

שילוב של Zero Trust, שרתי RAM בלבד ופרוטוקולים שנבדקו בביקורת.

Q2: מהם שרתי RAM בלבד?

שרתים הפועלים בזיכרון נדיף, שנועדו לא לשמור יומנים בדיסק.

Q3: מהו VPN מסוג Zero Trust?

מסגרת שמאמתת באופן רציף כל בקשת גישה וכל חיבור.

Q4: מדוע WireGuard נחשב מאובטח?

יש לו בסיס קוד קטן שקל לבצע בו ביקורת, והוא משתמש בצפנים מודרניים.

Q5: כיצד שירותי VPN מאובטחים מונעים דליפות DNS?

על ידי ניתוב כל השאילתות דרך פותרי DNS פרטיים ומוצפנים.

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

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

Q6: האם VPN מאובטח דורש ביקורות?

כן, ביקורות עצמאיות מאמתות טענות של אפס יומנים ואבטחת קוד.

Q7: מה תפקידו של kill switch?

הוא עוצר מיד את תעבורת הרשת אם חיבור ה-VPN מתנתק.

Q8: באיזו הצפנה משתמשים ב-VPN מאובטחים?

AES-256 ו-ChaCha20 הם תקני התעשייה להצפנה.

Q9: האם ניתוב Multi-Hop מאובטח?

כן, הוא משרשר שני שרתים או יותר כדי למנוע ניתוח תעבורה.

Q10: כיצד שיפוט אופשור עוזר?

הוא עשוי להגביל אילו חוקים חלים, אך אינו מציע חסינות מוחלטת.

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 שרתי RAM בלבד מונעים סיכוני תפיסת נתונים?

מכיוון שהם פועלים ב-RAM, ניתוק החשמל מוחק את הנתונים המוחזקים בזיכרון.

Q2: כיצד Zero Trust מחליף אבטחת היקף רגילה?

הוא מתייחס לכל לקוח כעוין ודורש אימות מתמשך.

Q3: מה הופך את בסיס הקוד של WireGuard לקל יותר לביקורת?

קוד ה-Linux שלו מכיל פחות מ-4,000 שורות, הרבה פחות ממערכות VPN טיפוסיות. [4]

Q4: כיצד DNSSEC מגן על שאילתות DNS?

הוא חותם על רשומות DNS כדי שמפענחים יוכלו לזהות תשובות מזויפות או ששונו.

Q5: כיצד Multi-Hop מסבך מתאם תעבורה?

על ידי הפרדת כתובות IP נכנסות ויוצאות בין ספקי אירוח שונים.

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

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

Q6: מדוע סמכויות שיפוט של Five Eyes מסוכנות עבור VPN?

המדינות החברות חולקות מודיעין ועשויות להשתמש בצווים משפטיים כדי לבקש נתוני משתמשים.

Q7: כיצד מיושם kill switch ברמת הליבה?

הוא משתמש בכללי חומת אש של המערכת (כמו iptables או WFP) כדי לחסום תעבורה יוצאת.

Q8: מהי סודיות מתקדמת בלחיצות יד של VPN?

הוא יוצר מפתחות הפעלה ייחודיים כך שלא ניתן לפענח הפעלות קודמות.

Q9: כיצד VPN מאובטחים מצמצמים דליפות WebRTC?

על ידי חסימת בקשות WebRTC או ניתובן דרך המנהרה.

Q10: כיצד ביקורות עצמאיות מבטיחות עמידה בפרטיות?

מבקרים מבצעים בדיקות חדירה ובוחנים תצורות שרתים.

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

שרתי RAM בלבד טוענים את מערכת ההפעלה שלהם לזיכרון בעת האתחול, כך שדבר אינו נשאר בדיסק לאחר הפעלה מחדש.

2. תובנות על VPN

WireGuard משתמש במסגרת Noise עם Curve25519, ChaCha20, Poly1305, BLAKE2s ו-HKDF. [3]

3. תובנות על VPN

Zero Trust מעניק גישה לכל משאב בנפרד ואינו נותן אמון משתמע על סמך מיקום ברשת (NIST SP 800-207). [1]

4. תובנות על VPN

ברית המודיעין Five Eyes כוללת את ארה"ב, בריטניה, קנדה, אוסטרליה וניו זילנד.

5. תובנות על VPN

דליפות WebRTC מתרחשות כשדפדפנים חושפים את כתובת ה-IP הציבורית האמיתית של הלקוח באמצעות שאילתות STUN.

6. תובנות על VPN

סודיות קדימה מושלמת (PFS) מבטיחה שחשיפת מפתח לטווח ארוך אינה חושפת מפתחות הפעלה קודמים. [3]

7. תובנה על VPN

Cure53, חברת אבטחה מברלין, פרסמה ביקורות של כמה ספקי VPN.

8. תובנה על VPN

דליפות DNS מתרחשות כאשר שאילתות DNS עוקפות את מנהרת ה-VPN ועוברות לשרתי השמות של ספק האינטרנט המקומי.

9. תובנה על VPN

שבבי RAM נדיפים דורשים אספקת חשמל רציפה כדי לשמור נתונים, ותכולתם אובדת עם כיבוי המכשיר.

10. תובנות על VPN

מערכות Zero Trust ארגוניות אוכפות בדיקות מצב מכשיר לפני מתן חיבור למשאבים מאובטחים. [1]

מקורות והפניות טכניים

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

מקורות אקדמיים ותעשייתיים

[1] NIST. (2020). SP 800-207: Zero Trust Architecture.
https://csrc.nist.gov/pubs/sp/800/207/final

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

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

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

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

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

מפתח תשובות: נקודת ביקורת 1 – שאלות אמריקאיות

1 **שרת RAM בלבד** RAM בלבד **תשובה נכונה: A**

הערה למורה

שרתי RAM בלבד אינם שומרים יומנים בדיסק ומוחקים נתונים באתחול מחדש. מקור: Most Secure VPN.

2 **שאלה 2** **תשובה נכונה: A**

הערה למורה

WireGuard משלב בסיס קוד קטן הניתן לביקורת עם צפנים מודרניים.

3 **מודל Zero Trust** אפס אמון **תשובה נכונה: A**

הערה למורה

מודלים של Zero Trust מאמתים באופן מתמשך את תאימות המכשיר לפני מתן גישה. ציטוט: Most Secure VPN.

4 **הגנת DNS** הגנת DNS **תשובה נכונה: A**

הערה למורה

הגנה מפני דליפות DNS מנתבת שאילתות חיפוש דרך מפענחים פרטיים. מקור: Most Secure VPN.

5 **מנהרות Multi-Hop** MULTI-HOP **תשובה נכונה: A**

הערה למורה

ניתוב Multi-Hop משרשר שני צמתי שרת נפרדים בטור. ציטוט: Most Secure VPN.

מפתח תשובות: נקודת ביקורת 2 – נכון או לא נכון

6 **שרת RAM בלבד** RAM בלבד

תשובה נכונה: נכון

הערה למורה

חומרת שרת RAM בלבד אינה כותבת נתונים לדיסק ונמחקת באתחול מחדש. מקור: Most Secure VPN.

7 **מהירות WireGuard** WIREGUARD

תשובה נכונה: נכון

הערה למורה

WireGuard משתמש בהצפנה מודרנית שנמנעת מצווארי בקבוק בעיבוד. מקור: Most Secure VPN.

8 **KILL SWITCH** מתג כשל בטוח

תשובה נכונה: נכון

הערה למורה

מתג חירום חוסם את כל התעבורה אם חיבור ה-VPN נופל. מקור: Most Secure VPN.

9 **ביקורות של צד שלישי** ביקורות חיוניות

תשובה נכונה: לא נכון

הערה למורה

ביקורות של צד שלישי חיוניות לאימות טענות הפרטיות של חברות. מקור: Most Secure VPN.

10 **שאלה 10**

תשובה נכונה: לא נכון

הערה למורה

Zero Trust אינו מעניק אמון מובלע על סמך מיקום ברשת.

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

C 1. Zero Trust	E 2. Multi-Hop	F 3. שרת RAM בלבד	G 4. הגנת DNS
H 5. KILL SWITCH	A 6. מערכת שנבדקה בביקורת	B 7. הצפנה	D 8. פרוטוקול

נקודת ביקורת 3: מפתח תשובות – מונחי מפתח

1 אפס אמון	2 ניתוב כפול	3 זיכרון בלבד	4 הגנת DNS
5 מתג הפסקה	6 מבוקר		

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

1 E – מתגהפסקה	2 D – שאילתות	3 B – ניתובכפול	4 H – פרוטוקול
5 G – הצפנה	6 C – זיכרוןבלבד	7 F – מבוקר	8 A – אפסאמון

הערות לדיון עבור מורים

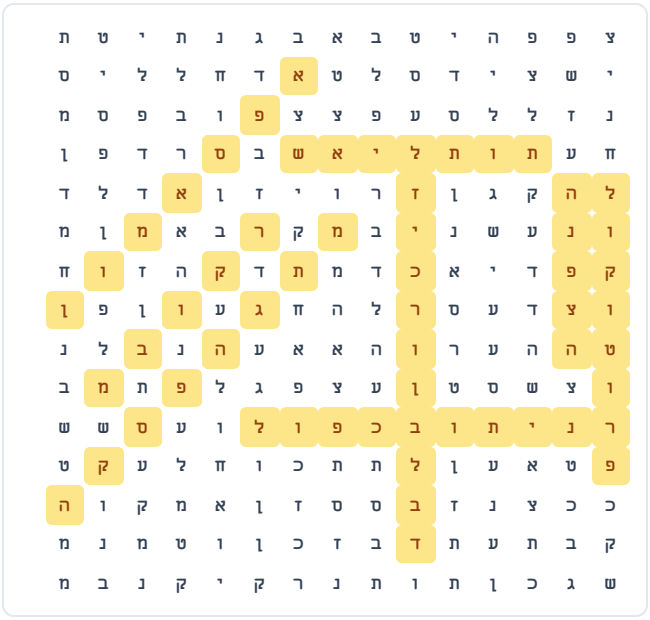
מונחי מפתח:
ודאו שהתלמידים מסבירים במילים שלהם את Zero Trust, Multi-Hop ו-שרת RAM בלבד ונותנים דוגמה לכל אחד מהם.

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

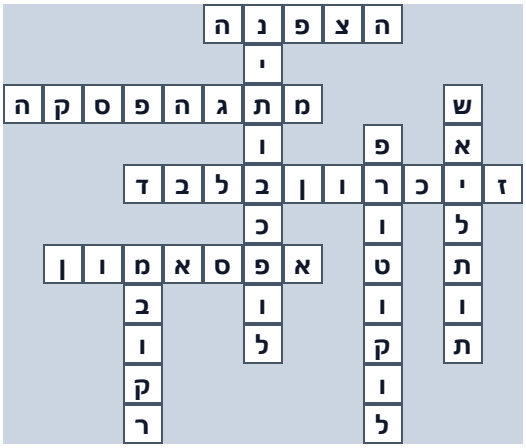
הערכת מקורות:
בקשו מהתלמידים לאמת לפחות טענה אחת במקורות של דף העבודה, ודונו מדוע נתונים, מחירים וכללים עשויים להשתנות עם הזמן.

מפתחות פאזלים והערות למורה

פתרון תפזורת



פתרון תשבץ



מדריך למורה לפתרונות התשבץ

מאוזן

1 מאוזן: הצפנה ערבול קריפטוגרפי של מטעני נתונים לאבטחת המעבר (5 אותיות)

4 מאוזן: מתגהפסקה מנגנון הגנה החוסם תעבורה אם ה-VPN נכשל (8 אותיות)

6 מאוזן: זיכרוןבלבד ארכיטקטורת שרתים המשתמשת בזיכרון נדיף לאחסון מטעני נתונים (10 אותיות)

7 מאוזן: אפסאמון מסגרת אבטחה הדורשת אימות מתמשך של כל המשתמשים (7 אותיות)

מאונך

2 מאונך: ניתובכפול ניתוב VPN במפל המשרשר שני צמתי שרת (9 אותיות)

3 מאונך: שאילתות אכיפת בקשות DNS פרטיות להגנה על חיפושי שרתי השמות (7 אותיות)

5 מאונך: פרוטוקול קבוצת כללים טכניים הקובעים כיצד נתונים נארזים ונשלחים (8 אותיות)

8 מאונך: מבוקר מערך שנבדק באופן עצמאי ומאשר שלא נשמרים יומנים (5 אותיות)

מפתח פתרונות: מילים מבולבלות ופענוח הצופן

מפתח הערכה לפעילות פענוח מילות אוצר המילים ולאתגר הצופן הסודי.

מפתח פענוח מילים מבולבלות

1. אואמנספ — **אפסאמון**
2. ברזיודבלכ — **זיכרונבלבד**
3. התמפסהקג — **מתגהפסקה**
4. פהנהצ — **הצפנה**
5. פבילכונות — **ניתובכפול**
6. ויתשלתא — **שאילתות**
7. קרמוב — **מבוקר**
8. טרולפוקו — **פרוטוקול**

מפתח אתגר הצופן הסודי

"אבטחה חזקה מגינה על נכסים יקרים"

מפתח תשובות למקרי הבוחן

A מקרה בוחן 1: חיזוק תשתית ארגונית

פתרון למורה

הנחיות הערכה

תשובות התלמידים צריכות לכלול את הנקודות הבאות:

- ניתוח תרחיש: בנק ארגוני מתכנן מחדש את טופולוגיית הגישה מרחוק שלו. הוא דורש ארכיטקטורת zero trust שמקשרת את כל מכשירי הלקוח לשרתים מאובטחים.
- אסטרטגיה ופתרון מומלצים: הנחיות להערכה: הסבירו ש-micro-segmentation (פילוח מיקרו) מגביל גישה למשאבים ספציפיים ומונע תנועה רוחבית של איומים אם מכשיר נפרץ.

B מקרה בוחן 2: הגנות של שרתי RAM-Only

פתרון למורה

הנחיות הערכה

תשובות התלמידים צריכות לכלול את הנקודות הבאות:

- ניתוח תרחיש: ספק VPN ממוקד אבטחה משדרג את השרתים שלו כדי למנוע שתפיסת שרת פיזית תחשוף היסטוריות יומני משתמשים.
- אסטרטגיה ופתרון מומלצים: הנחיות להערכה: פרטו ששרתי RAM-Only חסרים אחסון דיסק פיזי. אובדן מתח מוחק אוטומטית את כל הנתונים הזמניים בזיכרון הנדיף.