שם: _____ תאריך: _____ ציון: _____

אבטחה ב-ExpressVPN

הערכת תשתית האבטחה של ExpressVPN, פרוטוקול Lightway בקוד פתוח, טכנולוגיית TrustedServer ב-RAM בלבד, ביקורות אבטחה עצמאיות והגנת kill switch של Network Lock.

סקירת למידה: אבטחה ב-EXPRESSVPN

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 תכונות האבטחה של ExpressVPN. תחקרו פרוטוקולי קוד פתוח, צמתי שרת ב-RAM בלבד, צפנים ו-Kill Switch של Network Lock.

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/expressvpn/security/

מפת הלמידה שלכם: אבטחת ExpressVPN

- נתחו את הארכיטקטורה הטכנית וכללי ההגדרה של האבטחה של ExpressVPN.
- 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 EXPRESSVPN

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 פרוטוקולים בקוד פתוח וצמתי שרתים מבוססי RAM בלבד. ולסיום, פעילות הבונוס "חשבו מהר".

מערכי שרתי RAM בלבד ופרוטוקולי חיבור בקוד פתוח

ExpressVPN משתמשת בטכנולוגיית TrustedServer ב-RAM בלבד כדי למנוע רישומים מקומיים, בשילוב פרוטוקול Lightway בקוד פתוח ו-Internet Kill Switch, כדי לספק אבטחת נתוני משתמשים מקצה לקצה.

(מבוא)

ExpressVPN משתמשת בטכנולוגיית TrustedServer ב-RAM בלבד כדי למנוע רישומים מקומיים, בשילוב פרוטוקול Lightway בקוד פתוח ו-Internet Kill Switch, כדי לספק אבטחת נתוני משתמשים מקצה לקצה.

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

נקודת ביקורת 1: אתגר שאלות אמריקאיות

1 1. מהו הפרוטוקול הקוד-פתוח המותאם אישית של ExpressVPN?

- A) Lightway
- B) WireGuard
- C) OpenVPN
- D) Chameleon

2 2. איזו טכנולוגיית שרתים פועלת אך ורק בזיכרון RAM נדיף?

- A) TrustedServer
- B) RAM-Core
- C) SecureRAM
- D) שרת NoSpy

3 3. מה קורה אם חיבור VPN מתנתק באופן בלתי צפוי?

- A) מתג החירום חוסם את התעבורה
- B) התעבורה דולפת לספק האינטרנט
- C) המערכת מאתחלת
- D) הנתונים הופכים בלתי מוצפנים

4 4. היכן ExpressVPN רשומה כדי להגן על הפרטיות?

- A) איי הבתולה הבריטיים
- B) שווייץ
- C) פנמה
- D) רומניה

5 5. באיזה צופן סימטרי משתמשים כברירת מחדל?

- A) AES-256-GCM
- B) Blowfish
- C) DES-64
- D) RC4

נקודת ביקורת 2: אתגר נכון או לא נכון

שאלה 6

6. טכנולוגיית TrustedServer מאחסנת יומני שרת בכוננים קשיחים.

נכון לא נכון

שאלה 7

7. ExpressVPN עברה ביקורות אבטחה של צד שלישי.

נכון לא נכון

שאלה 8

8. פרוטוקול Lightway בנוי על בסיס הקוד של OpenVPN.

נכון לא נכון

שאלה 9

9. מתג החירום מופעל כברירת מחדל באפליקציות שולחן העבודה.

נכון לא נכון

שאלה 10

10. ExpressVPN מפעילה DNS פרטי בכל שרת ושרת.

נכון לא נכון

נקודת ביקורת 3: השלמת מונחי מפתח

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

1. הפרוטוקול המהיר שפיתחה ExpressVPN בעצמה הוא _____ .
2. כדי למנוע שמירת נתונים, רשת השרתים מסתמכת על צמתי RAM בלבד מסוג _____ .
3. מתג ההפסקה של ExpressVPN נקרא בעבר " _____ רשת".
4. ExpressVPN רשומה לפי חוקי _____ הבתולה הבריטיים.
5. מטעני הנתונים מאובטחים באמצעות צופן סימטרי חזק: _____ .
6. מדיניות אפס היומנים אומתה ועברה _____ עצמאית על ידי חברות מובילות.

בנק מילים

איי	ביקורת	דליפה	לייטוויי	נעילת	שרת מהימן	AES-256	DNS

כתבו את תשובותיכם כאן:

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

נקודת ביקורת 4: התאמת מושגים ב-VPN וברשתות

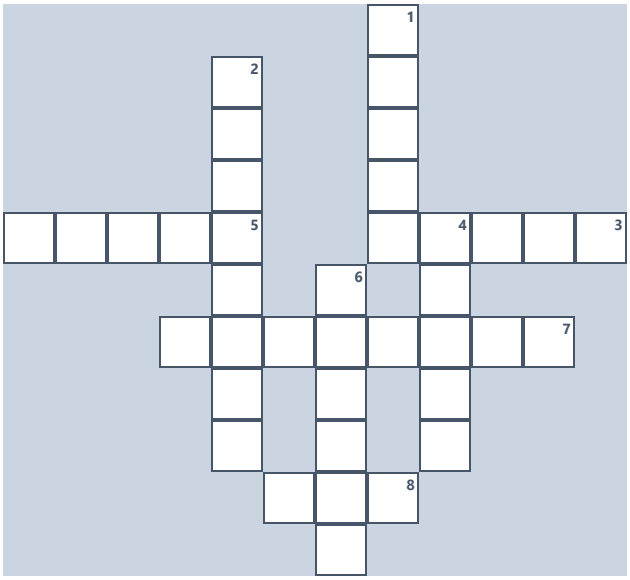
התאמת הגדרות

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

1. Lightway	A	סמכות השיפוט של איי הבתולה הבריטיים, המציעה פרטיות חזקה
2. TrustedServer	B	חשיפה לא מכוונת של נתוני IP, DNS או WebRTC פרטיים
3. נעילה	C	מפענחי מערכת שמות הדומיינים (DNS) פועלים באופן פרטי בכל צומת שרת
4. איים	D	אומת באופן עצמאי על ידי חברות אבטחה של צד שלישי
5. AES-256	E	ארכיטקטורת שרתים מסוג RAM בלבד המונעת אחסון נתונים בדיסק
6. נבדק	F	המילה האחרונה ב-Network Lock, השם הקודם של מתג החירום
7. דליפה	G	פרוטוקול חיבור קל משקל ובקוד פתוח של ExpressVPN
8. DNS	H	תקן הצפנה סימטרית המאבטח העברת נתונים

נקודת ביקורת 5: תשבץ

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



מאוזן

3. תקן סימטרי המאבטח את העברת הנתונים (5)

5. נבדק ואומת באופן עצמאי על ידי חברות אבטחה חיצוניות (5)

7. פרוטוקול חיבור קל משקל ובקוד פתוח של ExpressVPN (8)

8. שטח השיפוט של הבתולה הבריטית, המציע הגנת פרטיות חזקה (3)

מאונך

1. חשיפה בלתי מכוונת של נתוני IP, DNS או WebRTC פרטיים (5)

2. ארכיטקטורת שרתים המבוססת על RAM בלבד, המונעת אחסון נתונים בדיסק (8)

4. המילה הראשונה בשם Network Lock, שמו הקודם של מתג ההפסקה (5)

6. המערכת (DNS) שפותרי השמות שלה פועלים באופן פרטי בכל צומת שרת (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: תקן סימטרי המאבטח את העברת הנתונים (5 אותיות):

5 מאוזן: נבדק ואומת באופן עצמאי על ידי חברות אבטחה חיצוניות (5 אותיות):

7 מאוזן: פרוטוקול חיבור קל משקל ובקוד פתוח של ExpressVPN (8 אותיות):

8 מאוזן: שטח השיפוט של הבתולה הבריטית, המציע הגנת פרטיות חזקה (3 אותיות):

מאונך

1 מאונך: חשיפה בלתי מכוונת של נתוני IP, DNS או WebRTC פרטיים (5 אותיות):

2 מאונך: ארכיטקטורת שרתים המבוססת על RAM בלבד, המונעת אחסון נתונים בדיסק (8 אותיות):

4 מאונך: המילה הראשונה בשם Network Lock, שמו הקודם של מתג ההפסקה (5 אותיות):

6 מאונך: המערכת (DNS) שפותרי השמות שלה פועלים באופן פרטי בכל צומת שרת (6 אותיות):

נקודת ביקורת 6: חיפוש מילה נסתרת

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

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

רשימת מילים

לייטוויי | שרתמהימן | נעילה | איי | הצפנה | מבוקר | דליפה | דומיין

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. לייטוויי
B. שרתמהימן
C. נעילה
D. איי
E. הצפנה
F. מבוקר
G. דליפה
H. דומיין

	הגדרות ושדות התאמה
	1. חשיפה בלתי מכוונת של נתוני IP, DNS או WebRTC פרטיים.
	2. שטח השיפוט של הבתולה הבריטית, המציע הגנת פרטיות חזקה.
	3. המערכת (DNS) שפותרי השמות שלה פועלים באופן פרטי בכל צומת שרת.
	4. פרוטוקול חיבור קל משקל ובקוד פתוח של ExpressVPN.
	5. המילה הראשונה בשם Network Lock, שמו הקודם של מתג ההפסקה.
	6. תקן סימטרי המאבטח את העברת הנתונים.
	7. ארכיטקטורת שרתים המבוססת על RAM בלבד, המונעת אחסון נתונים בדיסק.
	8. נבדק ואומת באופן עצמאי על ידי חברות אבטחה חיצוניות.

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. יטולויי
2. נהליע
3. פההנצ
4. יהפדל
5. הירמשמת
6. יא
7. קרמוב
8. מנדיו

פעילות בונוס: חשבו מהר

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

1	תכונות שתחפשו ב-ExpressVPN			
2	איומים ברשתות Wi-Fi ציבוריות			
3	סוגי דליפות ב-VPN			
4	דרכים ליצור סיסמה חזקה			
5	כפתורים או תפריטים באפליקציית VPN			
6	דברים שאתם עושים באינטרנט בכל יום			
7	אנשים שהייתם ממליצים להם על ExpressVPN			
8	מדינות הידועות בחוקי פרטיות חזקים			
9	פרוטוקולי VPN שאתם מכירים			
10	דברים שביקורת (audit) יכולה לבדוק			
11	תכונות אבטחה ב-ExpressVPN			
12	דברים שכדאי לבדוק לפני רכישת VPN			
13	הגדרות שמפעילים לאבטחה נוספת			
14	דברים שהצפנה מגנה עליהם			
15	דברים ש-ExpressVPN יכול להסתיר מהרשת שלכם			

נקודת ביקורת 8: מקרי בוחן ב-VPN וברשתות

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

מקרה בוחן 1: אכיפת הגנות RAM-Only

👷

תרחיש: סוכנות ממשלתית תופסת שרת ExpressVPN כדי לחלץ יומני משתמשים והיסטוריית חיבורים.

שאלה לדיון: איזה מידע ימצאו בשרת, ומדוע?

מקרה בוחן 2: מנהרות חיבור Wi-Fi לא יציבות

👷

תרחיש: עובד מרחוק משתמש ב-Wi-Fi ציבורי במלון שמתנתק כל כמה דקות בזמן עריכת מסמכים.

שאלה לדיון: כיצד ExpressVPN מגנה על הנתונים שלהם מפני דליפה במהלך ניתוקים?

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

25	13	10	5	13		22	20	21		22	10	10	3	6	12	6	14	11	9

24	6	10	13	6	10		24	10	14	13	6	10		22	19	8	6	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 על רשתות פרטיות וירטואליות (VPN) ועל מנהור.

Q1: באיזו הצפנה ExpressVPN משתמשת?

ExpressVPN משתמשת כברירת מחדל בהצפנה סימטרית AES-256-GCM.

Q2: מהו פרוטוקול Lightway?

Lightway הוא פרוטוקול מותאם אישית של ExpressVPN, שנבנה למהירות, אבטחה ויציבות.

Q3: האם ExpressVPN מתעדת את היסטוריית החיפושים שלי?

לא, ExpressVPN אוכפת מדיניות קפדנית של אפס יומנים שעברה ביקורת עצמאית.

Q4: מהו Internet Kill Switch?

זהו kill switch המובנה של ExpressVPN שחוסם תעבורת אינטרנט אם החיבור מתנתק.

Q5: האם פרוטוקול Lightway הוא בקוד פתוח?

כן, הקוד המרכזי של פרוטוקול Lightway הוא קוד פתוח וזמין ב-[9] .GitHub

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

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

Q6: האם ExpressVPN מפעילה DNS פרטי?

כן, ExpressVPN מפעילה DNS פרטי ומוצפן משלה בכל שרת. [7]

Q7: מהי טכנולוגיית TrustedServer?

זוהי הגדרת שרת שבה מערכת ההפעלה והאפליקציות פועלות כולן בזיכרון RAM נדיף.

Q8: האם ExpressVPN עברה ביקורת?

כן, ExpressVPN נבדקה על ידי חברות כמו PwC, Cure53 ו-F-Secure. [1]

Q9: האם ExpressVPN מגינה מפני דליפות DNS ו-IPv6?

כן, Internet Kill Switch חוסם תעבורת IPv4, IPv6 ו-DNS מחוץ למנהרה.

Q10: היכן ExpressVPN ממוקמת?

ExpressVPN התאגדה באיי הבתולה הבריטיים (BVI).

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 ארכיטקטורת RAM בלבד משפרת אבטחה?

נתונים אינם נכתבים לכוננים קשיחים, ונתונים המוחזקים בזיכרון נמחקים בכל פעם שהשרת כבוי.

Q2: מדוע סמכות השיפוט של BVI חשובה לפרטיות?

ExpressVPN מבוססת ב-BVI, ולכן דרישות משפטיות לנתונים כפופות לחוקי BVI.

Q3: האם ExpressVPN תומכת בסודיות מתקדמת (perfect forward secrecy)?

כן, Lightway משתמש במפתחות דינמיים שנמחקים ונוצרים מחדש באופן קבוע.

Q4: כיצד Network Lock מונע דליפות IP?

הוא חוסם את כל התעבורה ברמת המערכת בכל פעם שחיבור ה-VPN מתנתק.

Q5: האם Lightway מגן מפני התקפות קוונטיות?

כן, ל-Lightway יש הגנה פוסט-קוונטית באמצעות תקן NIST ML-KEM.

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

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

Q6: האם גופי ממשל יכולים ליירט תעבורת Lightway?

הם יכולים ליירט אותו, אך אינם יכולים לפענח אותו בגלל הצפנת AES-256/ChaCha20.

Q7: כיצד DNS פרטי מגן על יומני החיפוש של המשתמש?

הוא מעבד את כל שאילתות ה-DNS בתוך המנהרה המוצפנת ומונע ניטור על ידי ספק האינטרנט.

Q8: למה משמש Lightway Turbo?

הוא משתמש במנהור רב-נתיבי כדי לשלוח יותר נתונים בבת אחת ולהשיג מהירויות גבוהות יותר.

Q9: מהו היתרון של Lightway על פני WireGuard?

Lightway נבנה במיוחד כדי לטפל במעברי רשת (כמו מ-Wi-Fi לרשת סלולרית) במהירות וללא ניתוק.

Q10: באיזו תדירות תוכנת השרת מותקנת מחדש?

עם TrustedServer, כל מחסנית התוכנה נטענת מחדש מתמונת קריאה בלבד מאובטחת בכל אתחול.

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

Lightway משתמש ב-AES-256-GCM, או ב-ChaCha20/Poly1305 במכשירים חלשי הספק. [6]

2. תובנות על VPN

טכנולוגיית TrustedServer נועדה להריץ את כל פעולות השרת ב-RAM. [4]

3. תובנות על VPN

איי הבתולה הבריטיים (BVI) משמשים כסמכות השיפוט התאגידית. [8]

4. תובנות על VPN

Lightway נכתב מחדש משפת C ל-Rust ועבר ביקורת של Cure53 ו-Praetorian. [3]

5. תובנות על VPN

Internet Kill Switch חוסם תעבורה ברמת המערכת אם ה-VPN מתנתק. [5]

6. תובנות על VPN

כל שאילתות ה-DNS נפתרות דרך שרתי DNS פרטיים ומוצפנים. [7]

7. תובנה על VPN

ExpressVPN פרסמה יותר מ-20 ביקורות עצמאיות של צד שלישי. [1]

8. תובנה על VPN

השירות אינו רושם כתובות IP, היסטוריית גלישה או מטא-נתוני תעבורה.

9. תובנה על VPN

סודיות קדימה מושלמת נשמרת באמצעות החלפה דינמית של מפתחות הפעלה. [1]

10. תובנות על VPN

פרוטוקול Lightway תומך הן בשכבת התעבורה UDP והן ב-TCP.

מקורות והפניות טכניים

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

מקורות אקדמיים ותעשייתיים

[1] ExpressVPN. (n.d.). ExpressVPN Trust Center.
https://www.expressvpn.com/trust

[2] ExpressVPN. (n.d.). Lightway: A VPN Protocol by ExpressVPN.
https://www.expressvpn.com/lightway

[3] ExpressVPN. (2025). Lightway's Rust rewrite undergoes two security audits, by Cure53 and Praetorian.
https://www.expressvpn.com/blog/lightway-audits-cure53-praetorian/

[4] ExpressVPN. (n.d.). ExpressVPN TrustedServer Technology.
https://www.expressvpn.com/features/trustedserver

[5] ExpressVPN. (n.d.). VPN Kill Switch: What It Is & How ExpressVPN Keeps You Safe.
https://www.expressvpn.com/features/network-lock

[6] ExpressVPN. (n.d.). How Secure Is VPN Encryption?
https://www.expressvpn.com/what-is-vpn/vpn-encryption

[7] ExpressVPN. (n.d.). Get a VPN With Private DNS.
https://www.expressvpn.com/features/dns

[8] ExpressVPN. (n.d.). ExpressVPN Privacy Policy.
https://www.expressvpn.com/privacy-policy

[9] ExpressVPN. (n.d.). Lightway Rust Open Source Workspace [GitHub repository].
https://github.com/expressvpn/lightway

[10] Cure53. (2024). Audit-Report ExpressVPN Lightway Protocol 10.-11.2024.
https://cure53.de/pentest-report_expressvpn-lightway_2024.pdf

[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] Nir, Y., & Langley, A. (2018). RFC 8439: ChaCha20 and Poly1305 for IETF Protocols.
https://www.rfc-editor.org/rfc/rfc8439

מפתח תשובות: נקודת ביקורת 1 – שאלות אמריקאיות

1 שאלה 1 — תשובה נכונה: A

הערה למורה

מהו הפרוטוקול הקוד-פתוח המותאם אישית של Lightway → ?ExpressVPN

2 שאלה 2 — תשובה נכונה: A

הערה למורה

איזו טכנולוגיית שרתים פועלת אך ורק בזיכרון RAM נדיף? → TrustedServer

3 שאלה 3 — תשובה נכונה: A

הערה למורה

מה קורה אם חיבור VPN מתנתק באופן בלתי צפוי? → A) מתג החירום חוסם את התעבורה

4 שאלה 4 — תשובה נכונה: A

הערה למורה

היכן ExpressVPN רשומה כדי להגן על הפרטיות? → איי הבתולה הבריטיים

5 שאלה 5 — תשובה נכונה: A

הערה למורה

באיזה צופן סימטרי משתמשים כברירת מחדל? → AES-256-GCM

מפתח תשובות: נקודת ביקורת 2 – נכון או לא נכון

6 שאלה 6

תשובה נכונה: לא נכון

הערה למורה

טכנולוגיית TrustedServer מאחסנת יומני שרת בכוננים קשיחים.

7 שאלה 7

תשובה נכונה: נכון

הערה למורה

ExpressVPN עברה ביקורות אבטחה של צד שלישי.

8 שאלה 8

תשובה נכונה: לא נכון

הערה למורה

פרוטוקול Lightway בנוי על בסיס הקוד של OpenVPN.

9 שאלה 9

תשובה נכונה: נכון

הערה למורה

מתג החירום מופעל כברירת מחדל באפליקציות שולחן העבודה.

10 שאלה 10

תשובה נכונה: נכון

הערה למורה

ExpressVPN מפעילה DNS פרטי בכל שרת ושרת.

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

G 1. Lightway	E 2. TrustedServer	F 3. נעילה	A 4. איים
H 5. AES-256	D 6. נבדק	B 7. דליפה	C 8. DNS

נקודת ביקורת 3: מפתח תשובות – מונחי מפתח

1 לייטוויי	2 שרת מהימן	3 נעילת	4 איי
5 AES-256	6 ביקורת		

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

1 G – דליפה	2 D – איי	3 H – דומיין	4 A – לייטוויי
5 C – נעילה	6 E – הצפנה	7 B – שרתמהימן	8 F – מבוקר

הערות לדיון עבור מורים

מונחי מפתח:
ודאו שהתלמידים מסבירים במילים שלהם את Lightway, TrustedServer ו-נעילה ונותנים דוגמה לכל אחד מהם.

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

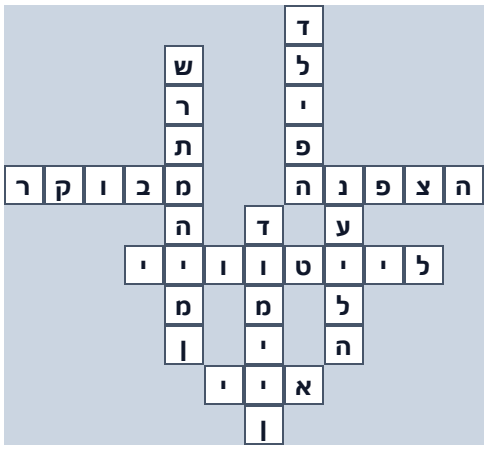
הערכת מקורות:
בקשו מהתלמידים לאמת לפחות טענה אחת במקורות של דף העבודה, ודונו מדוע נתונים, מחירים וכללים עשויים להשתנות עם הזמן.

מפתחות פאזלים והערות למורה

פתרון תפזורת

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

פתרון תשבץ



מדריך למורה לפתרונות התשבץ

מאוזן

3 מאוזן: הצפנה תקן סימטרי המאבטח את העברת הנתונים (5 אותיות)

5 מאוזן: מבוקר נבדק ואומת באופן עצמאי על ידי חברות אבטחה חיצוניות (5 אותיות)

7 מאוזן: לייטוויי פרוטוקול חיבור קל משקל ובקוד פתוח של ExpressVPN (8 אותיות)

8 מאוזן: איי שטח השיפוט של הבתולה הבריטית, המציע הגנת פרטיות חזקה (3 אותיות)

מאונך

1 מאונך: דליפה חשיפה בלתי מכוונת של נתוני IP, DNS או WebRTC פרטיים (5 אותיות)

2 מאונך: שרתמהימן ארכיטקטורת שרתים המבוססת על RAM בלבד, המונעת אחסון נתונים בדיסק (8 אותיות)

4 מאונך: נעילה המילה הראשונה בשם Network Lock, שמו הקודם של מתג ההפסקה (5 אותיות)

6 מאונך: דומיין המערכת (DNS) שפותרי השמות שלה פועלים באופן פרטי בכל צומת שרת (6 אותיות)

מפתח פתרונות: מילים מבולבלות ופענוח הצופן

מפתח הערכה לפעילות פענוח מילות אוצר המילים ולאתגר הצופן הסודי.

מפתח פענוח מילים מבולבלות

1. יטולויי — לייטוויי
2. נהליע — נעילה
3. פההנצ — הצפנה
4. יהפדל — דליפה
5. הירקמשמת — שרתמהימן
6. ייא — איי
7. קרמוב — מבוקר
8. מנדייו — דומיין

מפתח אתגר הצופן הסודי

"טכנולוגיית שרת מהימן מוחקת יומנים יומיום"

מפתח תשובות למקרי הבוחן

A מקרה בוחן 1: אכיפת הגנות RAM-Only

פתרון למורה

הנחיות הערכה

תשובות התלמידים צריכות לכלול את הנקודות הבאות:

- ניתוח תרחיש: סוכנות ממשלתית תופסת שרת ExpressVPN כדי לחלץ יומני משתמשים והיסטוריית חיבורים.
- אסטרטגיה ופתרון מומלצים: כלום. טכנולוגיית TrustedServer של ExpressVPN פועלת כולה ב-RAM, ולכן כל הנתונים נמחקים מיד עם אובדן מתח.

B מקרה בוחן 2: מנהרות חיבור Wi-Fi לא יציבות

פתרון למורה

הנחיות הערכה

תשובות התלמידים צריכות לכלול את הנקודות הבאות:

- ניתוח תרחיש: עובד מרחוק משתמש ב-Wi-Fi ציבורי במלון שמתנתק כל כמה דקות בזמן עריכת מסמכים.
- אסטרטגיה ופתרון מומלצים: Internet Kill Switch חוסם אוטומטית את כל תעבורת האינטרנט עד שמנהרת ה-VPN מוקמת מחדש.