שם: _____ תאריך: _____ ציון: _____

דף עבודה WireGuard לעומת OpenVPN

השוואת הפרוטוקולים WireGuard ו-OpenVPN, גודלי בסיס הקוד, מהירות ותקני הצפנה

סקירת למידה: VPN

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.

לומד

מעמד סטודנט

מסלול מגן הרשת

מאובטח

מצב חיבור

הגנה על מנות נתונים

פעיל

הגנה מפני דליפות

הגנה מפני דליפות DNS ו-IPv6

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

- השוו את מורכבות בסיס הקוד ואת מהירות הביקורת של פרוטוקולים.
- נתחו את שיפורי הביצועים של הרצה בתוך מרחב הליבה.
- השוו בין צפני OpenSSL להצפנה המודרנית של WireGuard.
- הגדרת זוגות מפתחות ציבורי ופרטי ללחיצות יד בין עמיתים.
- ניתוב תעבורת VPN דרך פורטי חומת אש של TCP ושל UDP.

הוראות לדף עבודה להשוואת פרוטוקולים

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 ביקורת של פרוטוקולים מודרניים. ולסיום, פעילות הבונוס "חשבו מהר".

WireGuard לעומת OpenVPN (מבוא)

בחירת פרוטוקול VPN מחייבת איזון בין מהירות לבין אפשרויות תצורה. OpenVPN הוא התקן במשך עשורים ומציע גמישות בתצורות TCP/UDP. WireGuard הוא תחליף מודרני הפועל ישירות במרחב הליבה עם 4,000 שורות קוד בלבד. הבנת ההבדלים בין הפרוטוקולים היא המפתח לייעול הרשתות המאובטחות שלכם.

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

נקודת ביקורת 1: אתגר שאלות אמריקאיות

1 1. מהו הגודל המשוער של בסיס הקוד של פרוטוקול WireGuard?

- A. כ-70,000 שורות
- B. מעל 100,000 שורות
- C. פחות מ-1,000 שורות
- D. כ-4,000 שורות

2 2. באיזה מרחב של מערכת ההפעלה רץ WireGuard?

- A. מרחב משתמש
- B. מרחב הליבה (Kernel space)
- C. מרחב האפליקציה
- D. מרחב וירטואלי

3 3. על איזו ספריית הצפנה OpenVPN מסתמך בעיקר?

- A. ChaCha20-Poly1305
- B. ספריית ההצפנה OpenSSL
- C. מסגרת הפרוטוקול Noise
- D. קידוד DES בטקסט גלוי

4 4. מהו יתרון ביצועים מרכזי של WireGuard על פני OpenVPN?

- A. לחיצות יד מהירות יותר בחיבור והשהיה נמוכה יותר
- B. עקיפת הצורך בכתובות IP ציבוריות
- C. תמיכה מובנית מקורית ב-dial-up ישן
- D. אפס תקורת סוללה במכשירים ניידים

5 5. כיצד WireGuard מאמת חיבורי עמיתים?

- A. על ידי החלפת סיסמאות משתמש רגילות
- B. על ידי אימות תעודות רישום דומיין
- C. על ידי שימוש בזוגות מפתחות ציבוריים ופרטיים סטטיים
- D. על ידי בדיקת מספרים סידוריים של חומרה

נקודת ביקורת 2: אתגר נכון או לא נכון

שאלה 6

6. בסיס הקוד הקומפקטי של WireGuard מקל משמעותית על הביקורת בו.

נכון לא נכון

שאלה 7

7. OpenVPN מהיר בדרך כלל יותר מ-WireGuard מפני שהוא פועל במרחב הגרעין.

נכון לא נכון

שאלה 8

8. OpenVPN ניתן להגדרה רחבה ותומך גם בפרוטוקולי UDP וגם בפרוטוקולי TCP.

נכון לא נכון

שאלה 9

9. WireGuard משתמש בהצפנה מודרנית כמו ChaCha20 להצפנה מהירה של חבילות.

נכון לא נכון

שאלה 10

10. WireGuard דורש הגדרות מורכבות של רשות אישורים לצורך אימות.

נכון לא נכון

נקודת ביקורת 3: השלמת מונחי מפתח

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

1. הפרוטוקול המודרני _____ פועל ישירות בתוך ליבת מערכת ההפעלה.
2. הפרוטוקול הישן _____ נשען על ספריית ההצפנה OpenSSL.
3. הרצת קוד בתוך _____ מפחיתה את תקורת החלפת ההקשר.
4. OpenVPN פועל בתוך _____ , ומנתב מנות דרך ממשקים וירטואליים.
5. WireGuard מזהה עמיתי חיבור באמצעות _____ ציבורי ופרטי.
6. גודל קטן של בסיס הקוד משפר את יכולת _____ האבטחה של התוכנה.

בנק מילים

ביקורת | ווירגארד | זוג מפתחות | מורשת OpenVPN | מרחב ליבה | מרחב משתמש | קוד קומפקטי

כתבו את תשובותיכם כאן:

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

נקודת ביקורת 4: התאמת מושגים ברשתות

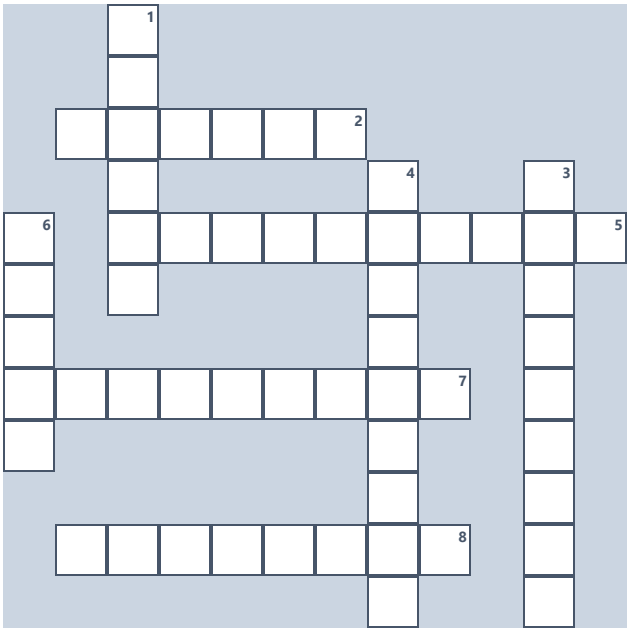
התאמת הגדרות

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. אזור הרצה שבו OpenVPN פועל, ויוצר תקורת החלפת הקשר.
2. OpenVPN		B. הגודל הקומפקטי של בסיס הקוד של WireGuard, שהופך אותו לקל הרבה יותר לביקורת.
3. מרחב ליבה		C. ספרייה קריפטוגרפית שעליה OpenVPN מסתמך עבור אלגוריתמי צפנים.
4. מרחב משתמש		D. פרוטוקולי תעבורה ש-OpenVPN תומך בהם; WireGuard עצמו פועל רק מעל UDP.
5. 4,000 שורות		E. אזור הרצה במערכת ההפעלה שבו WireGuard פועל לשם מהירות.
6. OpenSSL		F. אסימונים אסימטריים שבהם WireGuard משתמש כדי לאמת חיבורי עמיתים.
7. זוג מפתחות		G. פרוטוקול VPN מודרני שתוכנן למהירות גבוהה ולביקורת קוד פשוטה.
8. TCP/UDP		H. פרוטוקול ישן ויציב שמשתמש בבסיס קוד תצורה גדול ומורכב.

נקודת ביקורת 5: תשבץ

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



מאונך

1. מאגר קריפטוגרפי ש-OpenVPN נשען עליו עבור אלגוריתמי צופן (6)

3. אסימונים א-סימטריים שבהם WireGuard משתמש לאימות חיבורי עמיתים (9)

4. פרוטוקול VPN מודרני שתוכנן למהירות גבוהה ולביקורת קוד פשוטה (9)

6. פרוטוקול ותיק וחזק המשתמש בבסיס קוד גדול ומורכב של תצורה (5)

מאונן

2. פרוטוקולי העברה ש-OpenVPN תומך בהם; WireGuard עצמו רץ על UDP בלבד (6)

5. גודלו הקטן של בסיס הקוד של WireGuard, המקל מאוד על הביקורת (10)

7. אזור הרצה שבו OpenVPN פועל ויוצר תקורה של החלפת הקשר (9)

8. אזור הרצה במערכת ההפעלה שבו WireGuard פועל לשם מהירות (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: פרוטוקולי העברה ש-OpenVPN תומך בהם; WireGuard עצמו רץ על UDP בלבד (6 אותיות):

5 מאוזן: גודלו הקטן של בסיס הקוד של WireGuard, המקל מאוד על הביקורת (10 אותיות):

7 מאוזן: אזור הרצה שבו OpenVPN פועל ויוצר תקורה של החלפת הקשר (9 אותיות):

8 מאוזן: אזור הרצה במערכת ההפעלה שבו WireGuard פועל לשם מהירות (8 אותיות):

מאונך

1 מאונך: מאגר קריפטוגרפי ש-OpenVPN נשען עליו עבור אלגוריתמי צופן (6 אותיות):

3 מאונך: אסימונים א-סימטריים שבהם WireGuard משתמש לאימות חיבורי עמיתים (9 אותיות):

4 מאונך: פרוטוקול VPN מודרני שתוכנן למהירות גבוהה ולביקורת קוד פשוטה (9 אותיות):

6 מאונך: פרוטוקול ותיק וחזק המשתמש בבסיס קוד גדול ומורכב של תצורה (5 אותיות):

נקודת ביקורת 6: חיפוש מילה נסתרת

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

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

רשימת מילים

ווירגארד | מורשת | מרחבליבה | מרחבמשתמש תעבורה | קודקומפקטי | ספרייה | זוגמפתחות

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. מורשת
C. מרחבליבה
D. מרחבמשתמש
E. קודקומפקטי
F. ספרייה
G. זוגמפתחות
H. תעבורה

	הגדרות ושדות התאמה
	1. מאגר קריפטוגרפי ש-OpenVPN נשען עליו עבור אלגוריתמי צופן.
	2. אזור הרצה במערכת ההפעלה שבו WireGuard פועל לשם מהירות.
	3. פרוטוקול ותיק וחזק המשתמש בבסיס קוד גדול ומורכב של תצורה.
	4. אסימונים א-סימטריים שבהם WireGuard משתמש לאימות חיבורי עמיתים.
	5. פרוטוקולי העברה ש-OpenVPN תומך בהם; WireGuard עצמו רץ על UDP בלבד.
	6. גודלו הקטן של בסיס הקוד של WireGuard, המקל מאוד על הביקורת.
	7. פרוטוקול VPN מודרני שתוכנן למהירות גבוהה ולביקורת קוד פשוטה.
	8. אזור הרצה שבו OpenVPN פועל ויוצר תקורה של החלפת הקשר.

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. גריוואדי
2. בממרבילח
3. קמטפוויקקד
4. פתוממחתזוג
5. רתמשו
6. מברתשממשח
7. יסיהרפ
8. בהתרוע

פעילות בונוס: חשבו מהר

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

1. סיבות לבחור ב-WireGuard
2. הבטחות שספק VPN טוב מבטיח
3. סיבות לבחור ב-OpenVPN
4. סיבות להשתמש ב-VPN בזמן נסיעות
5. דברים שספק האינטרנט שלכם יכול לראות
6. דרכים לזהות רשת Wi-Fi מזויפת
7. מיתוסים על VPN
8. מקומות שבהם תשתמשו ב-VPN
9. דברים מהירים בחיי היום-יום
10. דברים ש-VPN לא יכול להגן עליכם מפניהם
11. דברים שמקלים על בדיקת קוד
12. דברים ש-VPN יכול להסתיר
13. הבדלים בין WireGuard ל-OpenVPN
14. מילים הקשורות לפרטיות
15. שמות של הצפנות שאתם מכירים

נקודת ביקורת 8: מקרי בוחן ב-VPN

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

שרה (סטודנטית בבית קפה)

👩‍💻 "היי! אני בבית הקפה והאפליקציית ה-VPN שלי מאפשרת לבחור WireGuard או OpenVPN. שיחות הווידאו שלי מתנתקות כשאני עוברת בין רשת בית הקפה לנקודה החמה של הטלפון. איזה פרוטוקול כדאי לבחור, ולמה הוא יתמודד טוב יותר עם המעבר?"

אלכס (סטודנט נוסע)

👨‍💻 "אני בחו״ל ברשת של מלון שנראה שחוסמת את רוב תעבורת ה-VPN. WireGuard לא מתחבר בכלל, אבל אני צריך לגשת למשאבי בית הספר שלי בארץ. מה כנראה נחסם, וכיצד OpenVPN יכול לעזור לי לעבור?"

נקודת ביקורת 9: פענוח הצופן

כדי להשלים את אימון ביקורת הפרוטוקולים שלכם, פענחו את ההודעה הנסתרת הזו על הרצה במרחב הליבה.

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

20	6	2	10	8	5		22	1		6	3	20	4	21
20	22	6	10		5	20	10	5	13		5	20	5	14	13	12

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 פרוטוקולים חשובים?

הפרוטוקול קובע כיצד ה-VPN שלכם בונה את המנהרה, איזו קריפטוגרפיה מגינה על הנתונים שלכם, ועד כמה מהר הוא מתחבר ומתחבר מחדש. WireGuard ו-OpenVPN הם שני הפרוטוקולים בקוד פתוח שרוב אפליקציות ה-VPN מציעות, והם מבצעים פשרות שונות בין פשטות, מהירות ויכולת הגדרה.

Q3: האם אחד מהם פרטי יותר מהאחר?

אף אחד מהפרוטוקולים אינו הופך אתכם לאנונימיים. שניהם מצפינים את תעבורת המנהרה בצפנים חזקים; הפרטיות שלכם תלויה בעיקר במה שספק ה-VPN רושם וכיצד הוא מנהל מפתחות, חשבונות ושרתים.

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 שניהם בקוד פתוח?

כן. WireGuard וגרסת הקהילה של OpenVPN מפרסמים את קוד המקור שלהם, כך שחוקרים עצמאיים יכולים לבדוק אותם. בסיס הקוד הקטן של WireGuard מאפשר בדיקה מלאה מהירה בהרבה.

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

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

Q6: איזה מהם מהיר יותר?

WireGuard מהיר בדרך כלל יותר: הוא פועל בקרנל, משתמש בהצפנת ChaCha20-Poly1305 רזה ומסיים לחיצות יד במהירות. ל-OpenVPN יש יותר תקורה, אך המהירויות בפועל תלויות גם בעומס השרת ובמרחק.

Q7: האם שניהם יכולים לפעול על TCP ועל UDP?

לא. OpenVPN יכול לפעול מעל UDP או TCP, ומצב TCP מסייע ברשתות החוסמות UDP. WireGuard שולח את החבילות שלו רק מעל UDP, ולכן הוא עלול להיכשל ברשתות המתירות רק TCP. [4]

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-WireGuard וב-OpenVPN בטלפון שלי?

כן. WireGuard הוא חוצה פלטפורמות, עם אפליקציות ל-Windows, macOS, Linux, iOS ו-Android, ולקוחות OpenVPN קיימים לאותן מערכות. רוב אפליקציות ה-VPN מאפשרות לבחור כל אחד מהם. [1]

Q10: מדוע WireGuard קטן כל כך?

WireGuard תומך בערכה קבועה אחת של צפנים מודרניים במקום באפשרויות רבות. המימוש שלו ב-Linux דורש פחות מ-4,000 שורות קוד, מה שמקל לבדוק אותו יותר מבסיסי קוד גדולים יותר של VPN. [3]

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: באילו צפנים משתמש WireGuard?

WireGuard משתמש ב-ChaCha20 עם Poly1305 להצפנה, ב-Curve25519 להחלפת מפתחות, ב-BLAKE2s לגיבוב ובמסגרת Noise ללחיצת היד. אין משא ומתן על צופן, ולכן משתמשים אינם יכולים לבחור אפשרות חלשה. [2]

Q3: באילו צפנים וספריות יכול OpenVPN להשתמש?

OpenVPN משולב באופן הדוק בספריית OpenSSL ומשתמש ב-TLS להחלפת מפתחות. מנהלי מערכת יכולים לבחור צפנים לערוץ הנתונים, כגון AES-256-GCM, מה שמוסיף גמישות אך גם מקום להגדרות חלשות. [4]

Q4: כיצד כל פרוטוקול מאמת עמיתים?

עמיתי WireGuard מזהים זה את זה לפי מפתחות ציבוריים סטטיים, בדומה להחלפת מפתחות SSH, וכל מפתח ממופה לכתובות IP מותרות במנהרה. OpenVPN מסתמך בדרך כלל על רשות אישורים עם אישורי X.509, ולעיתים קרובות בשילוב שם משתמש וסיסמה.

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: מה קורה כשאני עובר מ-Wi-Fi לרשת סלולרית?

WireGuard הוא חסר חיבור (connectionless): הוא שולח חבילות מהכתובת החדשה והמנהרה ממשיכה לפעול לאחר לחיצת יד מהירה. OpenVPN שומר מצב סשן, ולכן שינוי רשת עשוי לדרוש חיבור מחדש שנמשך מעט יותר.

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: האם OpenVPN עדיין בחירה טובה אם WireGuard מהיר יותר?

כן. OpenVPN בוגר ופרוס באופן נרחב, פועל על TCP כש-UDP חסום, ותומך בהגדרות ארגוניות מבוססות תעודות. ספקים רבים מציעים את שני הפרוטוקולים כדי שמשתמשים יוכלו להחליף אם אחד חסום או איטי.

Q9: באילו פורטים הם משתמשים?

הפורט הסטנדרטי של OpenVPN הוא 1194, אך אפשר להעביר אותו לכל פורט UDP או TCP, כולל 443. WireGuard מאזין לפורט UDP שנקבע בתצורה שלו; 51820 הוא הפורט המשמש בדוגמאות הרשמיות שלו.

Q10: איזה פרוטוקול קל יותר להגדרה ידנית?

WireGuard פשוט בדרך כלל יותר: יוצרים זוג מפתחות, מחליפים מפתחות ציבוריים ורושמים כתובות IP מותרות. OpenVPN דורש אישורים, CA ועוד אפשרויות, אם כי פרופילי .ovpn אורזים אותם בקובץ אחד.

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. שני אמצעי תעבורה

OpenVPN יכול להעביר את המנהרה שלו דרך UDP או TCP, ובמצב TLS ערוצי הבקרה והנתונים שלו חולקים פורט יחיד. [4]

3. מהפכת WIREGUARD

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

4. קריפטוגרפיה מודרנית

WireGuard משלב את ChaCha20, Poly1305, Curve25519, BLAKE2s, SipHash24 ו-HKDF בתוך מסגרת הפרוטוקול Noise, ללא בחירות צופן שהמשתמשים עלולים לטעות בהן. [2]

5. OPENSSL בתוך OPENVPN

OpenVPN משולב באופן הדוק בספריית OpenSSL ונסמך עליה לרבות מיכולותיו הקריפטוגרפיות, כולל TLS המשמש להחלפת מפתחות. [4]

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. מפתחות בסגנון SSH

חיבורי WireGuard נוצרים בהחלפת מפתחות ציבוריים פשוטים, בדומה להחלפת מפתחות SSH, ללא צורך ברשות אישורים. [1]

8. תמיכה בריבוי פלטפורמות

WireGuard שוחרר לראשונה עבור קרנל Linux וכיום זמין גם ל-Windows, macOS, BSD, iOS ו-Android, כך שאותו פרוטוקול פועל ברוב המכשירים. [1]

9. סודיות קדימה

WireGuard חוזר על לחיצת היד Noise_IK שלו כל כמה דקות כדי לסובב את מפתחות הסשן הסימטריים, ומספק סודיות קדימה מושלמת גם אם מפתח ארוך טווח ידלוף מאוחר יותר. [2]

10. ממשקי TUN/TAP

OpenVPN מתוכנן לעבוד עם ממשק הרשת הווירטואלי TUN/TAP, הזמין ברוב הפלטפורמות ונושא את חבילות המנהרה. [4]

מקורות והפניות טכניים

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

מקורות אקדמיים ותעשייתיים

[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] WireGuard. (n.d.). Quick Start.
https://www.wireguard.com/quickstart/

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

מפתח תשובות: השוואה בין פרוטוקולי WireGuard ו-OpenVPN, גודל בסיס הקוד, מהירות ותקני הצפנה

1 **גודל הקוד של WireGuard** פרוטוקולים

תשובה נכונה: D

הערה למורה

WireGuard קומפקטי במיוחד ופועל בכ-4,000 שורות קוד. כך שטח התקיפה נשאר קטן והביקורת קלה יותר. מקור: WireGuard Project.

2 **מהירות במרחב הגרעין** זמן השהיה

תשובה נכונה: B

הערה למורה

בזכות הרצה ישירות במרחב הליבה (kernel space), WireGuard נמנע מעומס החלפת הקשרים ומאפשר תפוקה גבוהה. ציטוט: WireGuard Project.

3 **שאלה 3**

תשובה נכונה: B

הערה למורה

OpenVPN משולב היטב עם OpenSSL, שמספקת צפנים כמו AES-GCM והופכת אותו לניתן להגדרה רבה אך מורכב יותר.

4 **ביצועי פרוטוקול** בקרות ניתוב

תשובה נכונה: A

הערה למורה

WireGuard יוצר לחיצות יד תוך אלפיות שנייה ומגיב מיד למעבר בין רשתות (למשל מעבר מ-Wi-Fi לסלולרי). מקור: Microsoft Native Gateway, Apple Support. [3]

5 **קריפטוגרפיה אסימטרית** פרטיות

תשובה נכונה: C

הערה למורה

WireGuard משתמש ב-Cryptokey Routing, המשייך מפתחות ציבוריים לכתובות IP מותרות במנהרה, בדומה להגדרות SSH. מקור: WireGuard Project.

מפתח תשובות: נקודת ביקורת 2 – נכון או לא נכון

6 שאלה 6

תשובה נכונה: נכון

הערה למורה

המימוש של WireGuard בלינוקס מתחת ל-4,000 שורות, ולכן צוותי אבטחה יכולים לסקור אותו מהר בהרבה מבסיסי קוד VPN גדולים בהרבה כמו OpenVPN.

7 השהיית מרחב משתמש מהירויות

תשובה נכונה: לא נכון

הערה למורה

OpenVPN פועל במרחב המשתמש ומעביר חבילות הלוך ושוב מהממשק הווירטואלי של הגרעין, מה שמוסיף עומס של החלפת הקשר (אלא אם משתמשים בהעברת עומס לגרעין כגון OpenVPN DCO). מקור: DD-WRT custom firmware.

8 תצורת OpenVPN סיכון האזנה

תשובה נכונה: נכון

הערה למורה

OpenVPN תומך בהרצה על גבי TCP (לאמינות/עקיפת חומות אש) או UDP (למהירות), ולכן הוא תואם לחומות אש ארגוניות מורכבות. מקור: IETF Cryptographic Protocols.

9 קריפטוגרפיה מודרנית חומות אש

תשובה נכונה: נכון

הערה למורה

WireGuard זונח צפנים ישנים לטובת רכיבים קריפטוגרפיים מודרניים ומאובטחים כמו ChaCha20 ו-Poly1305, הפועלים במהירות על מעבדים ניידים. מקור: WireGuard Project.

10 פישוט זוג המפתחות ללא יומנים

תשובה נכונה: לא נכון

הערה למורה

WireGuard אינו משתמש באישורים או בהיררכיות CA מורכבות; הוא מסתמך על זוגות מפתחות ציבורי/פרטי פשוטים המוחלפים בין העמיתים. מקור: WireGuard Project.

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. WireGuard	H 2. OpenVPN	E 3. מרחב ליבה	A 4. מרחב משתמש
B 5. 4,000 שורות	C 6. OpenSSL	F 7. זוג מפתחות	D 8. TCP/UDP

נקודת ביקורת 3: מפתח תשובות – מונחי מפתח

1 וויירגארד	2 OpenVPN	3 מרחב ליבה	4 מרחב משתמש
5 זוג מפתחות	6 ביקורת		

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

1 F – ספרייה	2 C – מרחבליבה	3 B – מורשת	4 G – זוגמפתחות
5 H – תעבורה	6 E – קודקומפקטי	7 A – וויירגארד	8 D – מרחבמשתמש

הערות לדיון עבור מורים

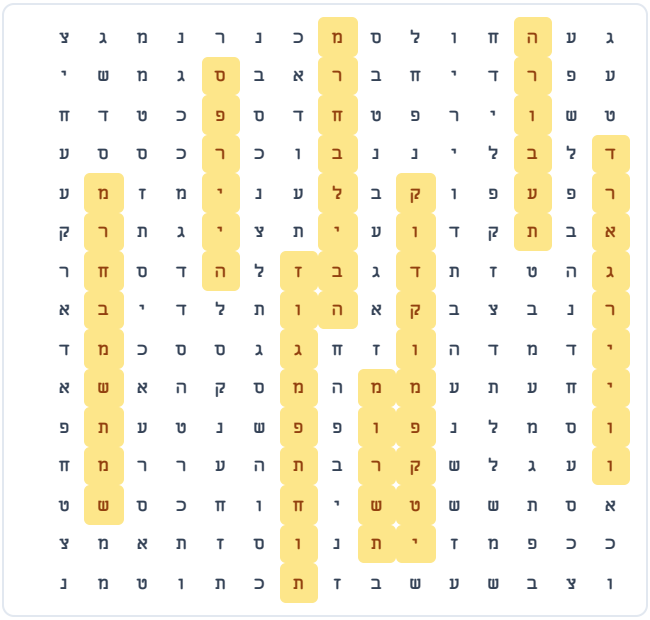
מונחי מפתח:
ודאו שהתלמידים מסבירים במילים שלהם את WireGuard, OpenVPN ו-מרחב ליבה ונותנים דוגמה לכל אחד מהם.

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

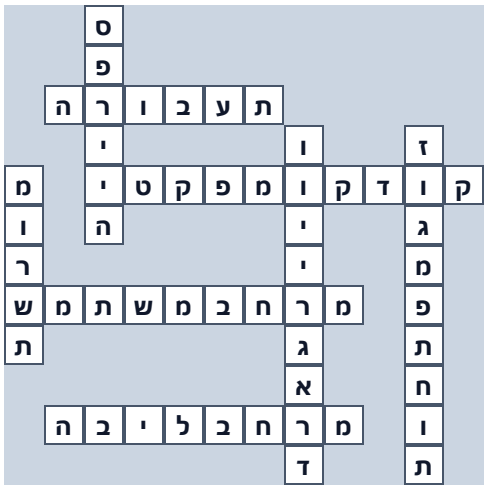
הערכת מקורות:
בקשו מהתלמידים לאמת לפחות טענה אחת במקורות של דף העבודה, ודונו מדוע נתונים, מחירים וכללים עשויים להשתנות עם הזמן.

מפתחות פאזלים והערות למורה

פתרון תפזורת



פתרון תשבץ



מדריך למורה לפתרונות התשבץ

מאוזן

2 מאוזן: תעבורה פרוטוקולי העברה ש-OpenVPN תומך בהם; WireGuard עצמו רץ על UDP בלבד (6 אותיות)

5 מאוזן: קודקומפקטי גודלו הקטן של בסיס הקוד של WireGuard, המקל מאוד על הביקורת (10 אותיות)

7 מאוזן: מרחבמשתמש אזור הרצה שבו OpenVPN פועל ויוצר תקורה של החלפת הקשר (9 אותיות)

8 מאוזן: מרחבליבה אזור הרצה במערכת ההפעלה שבו WireGuard פועל לשם מהירות (8 אותיות)

מאונך

1 מאונך: ספרייה מאגר קריפטוגרפי ש-OpenVPN נשען עליו עבור אלגוריתמי צופן (6 אותיות)

3 מאונך: זוגמפתחות אסימונים א-סימטריים שבהם WireGuard משתמש לאימות חיבורי עמיתים (9 אותיות)

4 מאונך: וויירגארד פרוטוקול VPN מודרני שתוכנן למהירות גבוהה ולביקורת קוד פשוטה (9 אותיות)

6 מאונך: מורשת פרוטוקול ותיק וחזק המשתמש בבסיס קוד גדול ומורכב של תצורה (5 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. במהרבילח — מרחבליבה
3. קמטפוויקקד — קודקומפקטי
4. פתומחתזוג — זוגמפתחות
5. רתמשו — מורשת
6. מברתשממשח — מרחבמשתמש
7. יסיהרפ — ספרייה
8. בהתרוע — תעבורה

מפתח אתגר הצופן הסודי

"שדרגו את החיבור למנהרה מהירה יותר"

מפתח תשובות למקרי הבוחן

A תרחיש A: בחירת פרוטוקול

האזנה והצפנה | הדילמה של שרה

הנחיות הערכה

תשובות התלמידים צריכות לכלול את הנקודות הבאות:

- המלצה: WireGuard. העיצוב הקל והחסר-חיבור שלו מאפשר למנהרה להתאושש במהירות כשהרשת שלה משתנה, ו-ChaCha20-Poly1305 שומר על הצפנה מהירה.
- אבטחה: שני הפרוטוקולים מצפינים את התעבורה שלה ברשת ה-Wi-Fi של בית הקפה, ולכן כל אחד מהם מגן על פרטי הכניסה שלה כשהוא מוגדר נכון; הבחירה משפיעה בעיקר על המהירות והיציבות.

B תרחיש B: עקיפת חסימות VPN

חסימה גאוגרפית וכתובות IP | הדילמה של אלכס

הנחיות הערכה

תשובות התלמידים צריכות לכלול את הנקודות הבאות:

- סיבת החסימה: WireGuard משתמש ב-UDP בלבד, וחומת האש של המלון כנראה חוסמת UDP או מזהה חבילות WireGuard באמצעות סינון או בדיקת חבילות עמוקה (DPI).
- כיצד OpenVPN עוזר: הוא יכול לפעול על TCP, כולל פורט 443 שבו משתמש HTTPS, ושחומות אש במלונות כמעט אינן חוסמות אותו לחלוטין כי גלישה באינטרנט תלויה בו.