שם: _____ תאריך: _____ ציון: _____

אבטחה ב-ProtonVPN

ניתוח ארכיטקטורת האבטחה של ProtonVPN, כולל שרתי Secure Core, סינון DNS של NetShield, סמכות שיפוט שווייצרית לפרטיות, אפליקציות בקוד פתוח שנבדקו בביקורת ופרוטוקול Stealth.

סקירת למידה: אבטחה ב-ProtonVPN

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 ארכיטקטורת האבטחה של Proton VPN. תחקרו שרתי Secure Core בבונקר, חסימת DNS של NetShield, חוקי פרטיות שווייצריים והסוואת Stealth.

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/protonvpn/security/

מפת הלמידה שלכם: אבטחת ProtonVPN

- נתחו את הארכיטקטורה הטכנית וכללי ההגדרה של האבטחה של ProtonVPN.
- 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 ProtonVPN

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 ניתוב כפול (double-hop) של Secure Core וממשל פרטיות שווייצרי. ולסיום, פעילות הבונוס "חשבו מהר".

ארכיטקטורת SECURE CORE בקפיצה כפולה ושיפוט הפרטיות השווייצי

Proton VPN מגן על תעבורת המשתמשים באמצעות שרתי Secure Core בבעלות Proton בשווייץ, באיסלנד ובשוודיה, אפליקציות בקוד פתוח שעברו ביקורת, ופרוטוקול הערפול Stealth שנועד לעקוף בדיקת חבילות עמוקה.

(מבוא)

Proton VPN מגן על תעבורת המשתמשים באמצעות שרתי Secure Core בבעלות Proton בשווייץ, באיסלנד ובשוודיה, אפליקציות בקוד פתוח שעברו ביקורת, ופרוטוקול הערפול Stealth שנועד לעקוף בדיקת חבילות עמוקה.

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

נקודת ביקורת 1: אתגר שאלות אמריקאיות

1 1. איזה סוג מתקנים מארחים את שרתי Secure Core של Proton?

- A) מכונות וירטואליות בענן ציבורי
- B) אתרים מאובטחים ברמה גבוהה
- C) מרכזי נתונים ציבוריים
- D) ארונות שרתים משותפים

2 2. איזה פרוטוקול עוזר לעקוף צנזורה ממשלתית מחמירה?

- A) PPTP
- B) פרוטוקול Stealth
- C) OpenVPN UDP
- D) IKEv2

3 3. מהי הפונקציה של תכונת NetShield של Proton VPN?

- A) Speed Booster
- B) חסימת פרסומות ונוזקות ברמת ה-DNS
- C) אחסון בענן
- D) העברת יציאות

4 4. תחת חוקי הפרטיות של איזו מדינה פועלת Proton AG?

- A) ארצות הברית
- B) הממלכה המאוחדת
- C) שווייץ
- D) פנמה

5 5. כיצד מומחים מאמתים את אפליקציות הלקוח של Proton VPN?

- A) קוד סודי
- B) ביקורות קוד פתוח
- C) רישיון קנייני
- D) ביקורת ממשלתית

נקודת ביקורת 2: אתגר נכון או לא נכון

שאלה 6

6. Secure Core מנתב את התעבורה דרך מדינות ידידותיות לפרטיות לפני היציאה.

נכון ○ לא נכון ○

שאלה 7

7. שווייץ היא חברה בברית המעקב המודיעיני 14 Eyes.

נכון ○ לא נכון ○

שאלה 8

8. NetShield חוסם פרסומות ודומיינים זדוניים ישירות ברמת ה-DNS.

נכון ○ לא נכון ○

שאלה 9

9. אפליקציות Proton VPN הן בקוד פתוח ב-100% ועברו ביקורת פומבית.

נכון ○ לא נכון ○

שאלה 10

10. פרוטוקול Stealth משתמש בכותרות WireGuard רגילות ללא הסוואה.

נכון ○ לא נכון ○

נקודת ביקורת 3: השלמת מונחי מפתח

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

1. ניתוב רב-קפיצות דרך שרתים בבעלות Proton במדינות ידידותיות לפרטיות נקרא ארכיטקטורת _____ מאובטחת.
2. כדי להתגבר על בדיקת מנות עמוקה ועל חומות אש ברשת, משתמשים מפעילים מצב _____ .
3. דומיינים של נוזקות, מעקבים וסקריפטים של פרסומות מסוננים על ידי DNS של _____ .
4. Proton מציינת שלפי _____ היא אינה מחויבת לשמור יומנים של פעילות משתמשים.
5. אם מנהרת ה-VPN מתנתקת באופן בלתי צפוי, תעבורת האינטרנט נחסמת על ידי מנגנון _____ .
6. חוקרי אבטחה עצמאיים מאמתים את שלמות הלקוח משום שהיישומים מפורסמים בתור _____ .

בנק מילים

וויירגארד | חוקי שווייץ | ליבה | מתג הפסקה Stealth | צופן | קוד פתוח | NetShield

כתבו את תשובותיכם כאן:

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

נקודת ביקורת 4: התאמת מושגים ב-VPN וברשתות

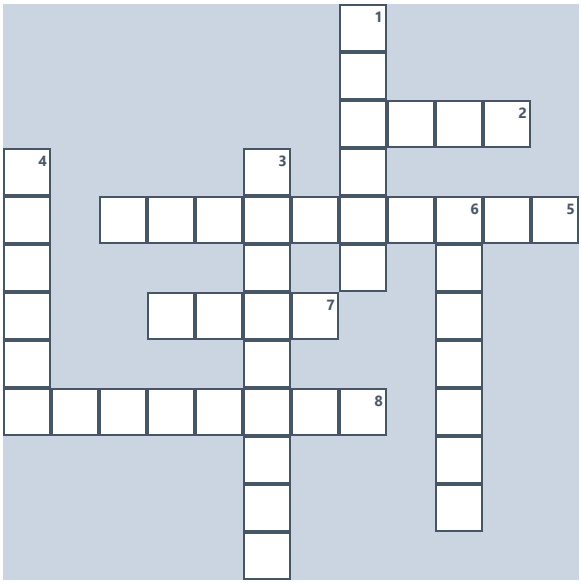
התאמת הגדרות

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

1. ליבה	A	תוכנת לקוח נגישה לציבור שעברה ביקורת עצמאית.
2. הסוואה	B	תקן צופן סימטרי המצפין את מנות הנתונים של ה-VPN.
3. מגן רשת	C	חוקי פרטיות קפדניים בשווייץ מחוץ לתחום השיפוט של 14 Eyes.
4. חוקי שווייץ	D	פרוטוקול מנהור מטושטש שמוסווה כתעבורת אינטרנט רגילה של HTTPS.
5. מתג הפסקה	E	פרוטוקול מודרני וקל משקל שמספק קריפטוגרפיה חזקה ומהירויות גבוהות.
6. קוד פתוח	F	מסנן מבוסס DNS שחוסם פרסומות, עוקבי טלמטריה ונוזקות.
7. וויירגארד	G	תכנון רב-דילוגי המנתב תעבורה דרך שרתי דילוג ראשון בבעלות Proton.
8. צופן	H	אמצעי הגנה שעוצר שידור ברשת בעת ניתוקי חיבור.

נקודת ביקורת 5: תשבץ

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



מאוזן

2. אלגוריתם סימטרי ברמה צבאית המאבטח את כל מנות ה-VPN העטופות (4)

5. חוקי פרטיות קפדניים בשווייץ מחוץ לתחום השיפוט של 14 העיניים (10)

7. תכנון רב-קפיצות המנתב תעבורה דרך שרתים בבעלות Proton כקפיצה ראשונה (4)

8. הגנת אבטחה העוצרת את שידור הרשת בעת ניתוקי חיבור (8)

מאונך

1. מסנן מבוסס DNS החוסם פרסומות, מעקבי טלמטריה ונוזקות (6)

3. פרוטוקול מודרני וקל משקל המספק הצפנה חזקה ומהירויות גבוהות (9)

4. פרוטוקול מנהור מוסווה, המחופש לתעבורת רשת HTTPS רגילה (6)

6. תוכנת יישום לקוח הנגישה לציבור ושנבדקה באופן עצמאי (7)

נקודת ביקורת 5 – פעילות חלופית: רמזים נגישים לתשבץ

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

מאוזן

2 מאוזן: אלגוריתם סימטרי ברמה צבאית המאבטח את כל מנות ה-VPN העטופות (4 אותיות):

5 מאוזן: חוקי פרטיות קפדניים בשווייץ מחוץ לתחום השיפוט של 14 העיניים (10 אותיות):

7 מאוזן: תכנון רב-קפיצות המנתב תעבורה דרך שרתים בבעלות Proton כקפיצה ראשונה (4 אותיות):

8 מאוזן: הגנת אבטחה העוצרת את שידור הרשת בעת ניתוקי חיבור (8 אותיות):

מאונך

1 מאונך: מסנן מבוסס DNS החוסם פרסומות, מעקבי טלמטריה ונוזקות (6 אותיות):

3 מאונך: פרוטוקול מודרני וקל משקל המספק הצפנה חזקה ומהירויות גבוהות (9 אותיות):

4 מאונך: פרוטוקול מנהור מוסווה, המחופש לתעבורת רשת HTTPS רגילה (6 אותיות):

6 מאונך: תוכנת יישום לקוח הנגישה לציבור ושנבדקה באופן עצמאי (7 אותיות):

נקודת ביקורת 6: חיפוש מילה נסתרת

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

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

רשימת מילים

ליבה | הסוואה | מגרשת | חוקישווייץ | מתגהפסקה | קודפתוח | ווירגארד | צופן

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. ליבה
B. הסוואה
C. מגרשת
D. חוקישווייץ
E. מתגהפסקה
F. קודפתוח
G. וויירגארד
H. צופן

	הגדרות ושדות התאמה
	1. פרוטוקול מנהור מוסווה, המחופש לתעבורת רשת HTTPS רגילה.
	2. פרוטוקול מודרני וקל משקל המספק הצפנה חזקה ומהירויות גבוהות.
	3. חוקי פרטיות קפדניים בשווייץ מחוץ לתחום השיפוט של 14 העיניים.
	4. תכנון רב-קפיצות המנתב תעבורה דרך שרתים בבעלות Proton כקפיצה ראשונה.
	5. אלגוריתם סימטרי ברמה צבאית המאבטח את כל מנות ה-VPN העטופות.
	6. הגנת אבטחה העוצרת את שידור הרשת בעת ניתוקי חיבור.
	7. מסנן מבוסס DNS החוסם פרסומות, מעקבי טלמטריה ונוזקות.
	8. תוכנת יישום לקוח הנגישה לציבור ושנבדקה באופן עצמאי.

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. בלהי
2. תמנשרג
3. התמפסהקג
4. רדריאגווי
5. וווהאס
6. ישיויחווקק
7. קותחופד
8. צנפו

פעילות בונוס: חשבו מהר

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

1	דברים שאתם עושים באינטרנט בכל יום		
2	מדינות הידועות בחוקי פרטיות חזקים		
3	תכונות אבטחה ב-Proton VPN		
4	סוגי דליפות ב-VPN		
5	מצבים שבהם מתג חירום (kill switch) עוזר		
6	דברים שביקורת (audit) יכולה לבדוק		
7	הגדרות שמפעילים לאבטחה נוספת		
8	דברים שהצפנה מגנה עליהם		
9	מילים שמתארות אפליקציית VPN טובה		
10	סיבות לבחור ב-Proton VPN		
11	כפתורים או תפריטים באפליקציית VPN		
12	שירותי סטרימינג שאתם צופים בהם		
13	איומים ברשתות Wi-Fi ציבוריות		
14	דרכים ליצור סיסמה חזקה		
15	מדינות שתרצו בהן שרתים של Proton VPN		

נקודת ביקורת 8: מקרי בוחן ב-VPN וברשתות

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

מקרה בוחן 1: עקיפת חומות אש מגבילות



תרחיש: משתמש נוסע למדינה שבה תעבורת VPN רגילה כמו OpenVPN ו-WireGuard נחסמת על ידי DPI.

שאלה לדיון: איזו תצורת פרוטוקול של Proton VPN מאפשרת למשתמש לעקוף בדיקה ברמת מדינה?

מקרה בוחן 2: הגנה מפני יריבים מתקדמים



תרחיש: מבקר פיננסי חושד שצומת היציאה של ספק האינטרנט המקומי שלו עלול להיות מנוצל על ידי איומים מתמשכים מתקדמים.

שאלה לדיון: כיצד Secure Core מגן על זהות המבקר מפני פגיעה בצומת יציאה?

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

22	8	9	2	6	1	13		5	2	10	12		10	22	20	21			
	24	10	14	6	22	14		12	16		24	10	14	3	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: מהו Proton VPN Secure Core?

Secure Core מנתב את התעבורה דרך מספר שרתים במדינות ידידותיות לפרטיות לפני היציאה.

Q2: מהו פרוטוקול Stealth?

Stealth הוא פרוטוקול מוסווה המסתיר חיבורי VPN כתעבורת TLS/HTTPS רגילה.

Q3: כיצד NetShield מגן על משתמשים?

NetShield הוא כלי מבוסס DNS החוסם אוטומטית פרסומות, כלי מעקב ודומיינים של נוזקות.

Q4: האם Proton VPN מוגנת משפטית בשווייץ?

כן, בשווייץ יש חוקי פרטיות מחמירים והיא נמצאת מחוץ לסמכות השיפוט של ארה"ב ושל ברית ה-EU/14-Eyes. [4]

Q5: האם אפליקציות Proton VPN הן בקוד פתוח?

כן. האפליקציות של Proton VPN הן קוד פתוח ועברו ביקורות אבטחה שפורסמו.

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

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

Q6: באילו צפני הצפנה משתמשים?

Proton VPN משתמש ב-AES-256-GCM או ב-ChaCha20-Poly1305 עם HMAC-SHA384 ולחיצות יד של RSA-4096.

Q7: האם ל-Proton VPN יש Kill Switch?

כן, Proton VPN כוללת Kill Switch רגיל ו-Kill Switch קבוע כדי למנוע דליפות לא מוצפנות.

Q8: האם Proton VPN יכול להדליף שאילתות DNS?

לא, כל שאילתות ה-DNS מנותבות דרך שרתי DNS פרטיים מוצפנים בבעלות Proton.

Q9: האם Proton VPN שומרת יומני חיבור?

לא, Proton VPN שומרת על מדיניות קפדנית של אי-רישום, המאושרת בביקורות שנתיות של Securitum. [3]

Q10: האם Proton VPN פגיע לדליפות WebRTC?

לא, לקוחות Proton כוללים כללי חומת אש וכללי ניתוב מובנים החוסמים דליפות WebRTC.

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

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

Q1: היכן ממוקמים פיזית מרכזי הנתונים של Secure Core?

הם נמצאים בשווייץ, בבסיס צבאי לשעבר באיסלנד ובאתר תת-קרקעי בשוודיה. [1]

Q2: כיצד Perfect Forward Secrecy פועלת ב-Proton VPN?

מפתח הצפנה זמני וייחודי נוצר לכל הפעלה, ומונע פענוח למפרע.

Q3: מהו Permanent Kill Switch ב-Windows/Linux?

Kill Switch קבוע חוסם את כל תעבורת הרשת גם אם אפליקציית ה-VPN נסגרת לחלוטין או קורסת.

Q4: האם Proton VPN תומך בניתוב IPv6 ובהגנה מפני דליפות?

Proton VPN מנתב תעבורת IPv6 במלואה דרך מנהרות או משבית אותה בבטחה כדי למנוע דליפות.

Q5: כיצד סינון DNS של NetShield מתמודד עם בדיקת HTTPS?

NetShield פועל אך ורק בשכבת פענוח ה-DNS, ללא צורך בפענוח TLS פולשני.

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

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

Q6: מי ביצע את ביקורות הקוד של צד שלישי של Proton VPN?

SEC Consult ביקרה את האפליקציות, ו-Securitum מבקרת את האפליקציות ואת מדיניות ה-no-logs.

Q7: איך פרוטוקול Stealth משתווה ל-OpenVPN XOR או ל-Shadowsocks?

Stealth מנהר את WireGuard דרך TLS מוסווה ומציג ביצועים טובים יותר מהסוואה ישנה מבוססת OpenVPN. [5]

Q8: האם הרשויות השווייצריות יכולות לחייב את Proton VPN לתעד תעבורה?

Proton מציינת שלפי החוק השווייצרי אין היא מחויבת לשמור לוגים של פעילות או נתונים של משתמשים.

Q9: כיצד שרתי Proton VPN מוגנים מפני תפיסה?

כל שרתי Proton VPN הם מכונות bare-metal המוגנות בהצפנת דיסק מלאה. [2]

Q10: האם Proton VPN תומך בהגדרות שרת DNS מותאמות אישית?

כן, מנויים בתשלום יכולים להגדיר שרתי DNS upstream מותאמים אישית ישירות בהעדפות האפליקציה.

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

1. Proton מחזיקה ומתקינה בעצמה את שרתי Secure Core שלה באתרים בעלי אבטחה גבוהה בשווייץ, באיסלנד ובשוודיה. [1]

2. תובנות על VPN

2. אפליקציות הלקוח של Proton VPN הן בקוד פתוח ועוברות ביקורות קוד חוזרות של צד שלישי.

3. תובנות על VPN

3. פרוטוקול ההסוואה Stealth עוקף בדיקת מנות עמוקה על ידי הדמיית תעבורת TLS רגילה.

4. תובנות על VPN

4. שווייץ נמצאת מחוץ לבריתות שיתוף המודיעין הבינלאומיות 5-Eyes, 9-Eyes ו-14-Eyes. [4]

5. תובנות על VPN

5. NetShield פועל ברמת פותר ה-DNS ומונע פרסומות ונוזקות לפני הורדת המטען.

6. תובנות על VPN

6. Perfect Forward Secrecy מבטיחה שמפתחות שנפגעו אינם יכולים לפענח הפעלות תעבורה שנלכדו בעבר. [7]

7. תובנה על VPN

7. Proton VPN משתמשת בהצפנת דיסק מלאה בשרתי bare-metal כדי להגן על הגדרות השרתים. [2]

8. תובנה על VPN

8. מתג החירום הקבוע מונע דליפות נתונים לא מוצפנים גם בזמן הפעלה מחדש של מערכת ההפעלה.

9. תובנה על VPN

9. Securitum ביקרה ואישרה את מדיניות אי-הרישום של Proton VPN בחמישה ביקורות שנתיות רצופות. [3]

10. תובנות על VPN

10. Proton VPN פותחה על ידי מדענים שנפגשו ב-CERN (הארגון האירופי למחקר גרעיני). [4]

מקורות והפניות טכניים

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

מקורות אקדמיים ותעשייתיים

[1] Proton VPN. (n.d.). What is Secure Core?
https://protonvpn.com/support/secure-core-vpn

[2] Proton VPN. (n.d.). Proton VPN features.
https://protonvpn.com/features

[3] Proton VPN. (n.d.). Proton VPN passes 5th annual external audit of no-logs policy.
https://protonvpn.com/blog/no-logs-audit

[4] Proton VPN. (n.d.). Get a VPN protected by Swiss privacy laws.
https://protonvpn.com/features/swiss-based

[5] Proton VPN. (2022). Defeat censorship with Stealth, our new VPN protocol.
https://protonvpn.com/blog/stealth-vpn-protocol

[6] GitHub. (n.d.). ProtonVPN · GitHub.
https://github.com/ProtonVPN

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

[8] IETF. (2018). RFC 8439: ChaCha20 and Poly1305 for IETF Protocols.
https://www.rfc-editor.org/rfc/rfc8439

[9] NIST. (2007). SP 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC.
https://csrc.nist.gov/pubs/sp/800/38/d/final

[10] IETF. (2014). RFC 7359: Layer 3 Virtual Private Network (VPN) Tunnel Traffic Leakages in Dual-Stack Hosts/Networks.
https://www.rfc-editor.org/rfc/rfc7359

[11] IETF. (2021). RFC 9076: DNS Privacy Considerations.
https://www.rfc-editor.org/rfc/rfc9076

[12] Federal Data Protection and Information Commissioner. (n.d.). Federal Data Protection and Information Commissioner (FDPIC).
https://www.edoeb.admin.ch/en

מפתח תשובות: נקודת ביקורת 1 – שאלות אמריקאיות

1 שאלה 1

תשובה נכונה: B

הערה למורה

שרתי Secure Core ממוקמים באתרים מאובטחים ברמה גבוהה, כולל בסיס צבאי לשעבר באיסלנד ומרכז נתונים תת-קרקעי בשוודיה.

2 פרוטוקול הסוואה Stealth

הגנה מפני צנזורה

תשובה נכונה: B

הערה למורה

פרוטוקול Stealth של Proton מסווה חיבורי WireGuard כתעבורת TLS/HTTPS רגילה כדי לעקוף חומות אש של בדיקת חבילות עמוקה (DPI). מקור: Proton Stealth Protocol Whitepaper.

3 חוסם פרסומות DNS של NetShield

סינון DNS

תשובה נכונה: B

הערה למורה

NetShield משתמש בסינון ברמת ה-DNS כדי לחסום דומיינים של נוזקות, תוכנות ריגול, פרסום פולשני ומעקבי טלמטריה לפני טעינת דפי האינטרנט. ציטוט: NetShield Security Specs.

4 תחום שיפוט משפטי שווייצרי

שיפוט

תשובה נכונה: C

הערה למורה

Proton AG שוכנת בז'נבה, שווייץ, ונהנית מחוקי פרטיות שווייצריים חזקים מחוץ לבריתות המעקב 14 Eyes של ארה"ב והאיחוד האירופי. מקור: Swiss Federal Data Protection Act. [4]

5 שאלה 5

תשובה נכונה: B

הערה למורה

כל אפליקציות Proton VPN הן בקוד פתוח; SEC Consult ובהמשך Securitum ביצעו עליהן ביקורת.

מפתח תשובות: נקודת ביקורת 2 – נכון או לא נכון

6 Secure Core רב-תחומי שיפוט
ארכיטקטורת ניתוב

תשובה נכונה: נכון

הערה למורה

Secure Core מנתב את התעבורה דרך תחומי שיפוט מוקשחי פרטיות לפני היציאה אל מדינת היעד, ובכך עוזר להגן מפני שרת יציאה שנפרץ. מקור: Secure Core Architecture.

7 ברית מעקב שווייצרית
בריתות מעקב

תשובה נכונה: לא נכון

הערה למורה

שווייץ אינה חברה בהסכמי שיתוף המודיעין 5 Eyes, 9 Eyes או 14 Eyes, ובכך שומרת על ריבונות משפטית עצמאית. מקור: International Surveillance Treaties.

8 שאלה 8

תשובה נכונה: נכון

הערה למורה

NetShield משתמש בשרתי ה-DNS של Proton כדי לבדוק דומיינים מול רשימות של דומיינים ידועים של פרסומות, עוקבים ונוזקות.

9 ביקורת על לקוח בקוד פתוח
שקיפות אבטחה

תשובה נכונה: נכון

הערה למורה

Proton הפכה את אפליקציות שולחן העבודה והנייד שלה לקוד פתוח ומפרסמת דוחות ביקורת של צד שלישי. מקור: SEC Consult Security Report.

10 שאלה 10

תשובה נכונה: לא נכון

הערה למורה

לא נכון: Stealth מנהר את WireGuard בתוך TLS מוסווה מעל TCP כך שהתעבורה נראית כ-HTTPS רגיל.

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. ליבה	D 2. הסוואה	F 3. מגן רשת	C 4. חוקי שווייץ
H 5. מתג הפסקה	A 6. קוד פתוח	E 7. ווירגארד	B 8. צופן

נקודת ביקורת 3: מפתח תשובות – מונחי מפתח

1 ליבה	2 Stealth	3 NetShield	4 חוקי שווייץ
5 מתג הפסקה	6 קוד פתוח		

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

1 B – הסוואה	2 G – ווירגארד	3 D – חוקישווייץ	4 A – ליבה
5 H – צופן	6 E – מתגהפסקה	7 C – מגרשת	8 F – קודפתוח

הערות לדיון עבור מורים

מונחי מפתח:
ודאו שהתלמידים מסבירים במילים שלהם את ליבה, הסוואה ו-מגן רשת ונותנים דוגמה לכל אחד מהם.

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

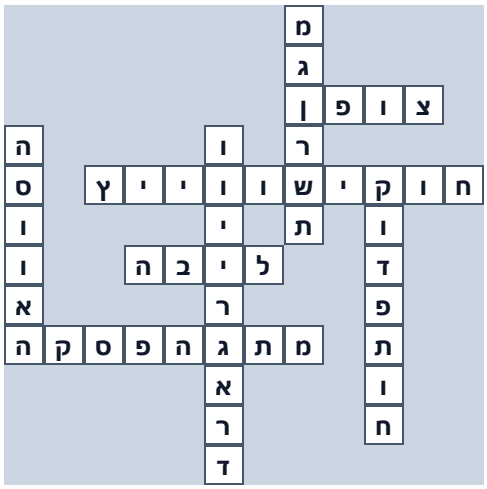
הערכת מקורות:
בקשו מהתלמידים לאמת לפחות טענה אחת במקורות של דף העבודה, ודונו מדוע נתונים, מחירים וכללים עשויים להשתנות עם הזמן.

מפתחות פאזלים והערות למורה

פתרון תפזורת

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

פתרון תשבץ



מדריך למורה לפתרונות התשבץ

מאוזן

2 מאוזן: צופן אלגוריתם סימטרי ברמה צבאית המאבטח את כל מנות ה-VPN העטופות (4 אותיות)

5 מאוזן: חוקישווייץ חוקי פרטיות קפדניים בשווייץ מחוץ לתחום השיפוט של 14 העיניים (10 אותיות)

7 מאוזן: ליבה תכנון רב-קפיצות המנתב תעבורה דרך שרתים בבעלות Proton כקפיצה ראשונה (4 אותיות)

8 מאוזן: מתגהפסקה הגנת אבטחה העוצרת את שידור הרשת בעת ניתוקי חיבור (8 אותיות)

מאונך

1 מאונך: מגרשת מסנן מבוסס DNS החוסם פרסומות, מעקבי טלמטריה ונוזקות (6 אותיות)

3 מאונך: ווייראגארד פרוטוקול מודרני וקל משקל המספק הצפנה חזקה ומהירויות גבוהות (9 אותיות)

4 מאונך: הסוואה פרוטוקול מנהור מוסווה, המחופש לתעבורת רשת HTTPS רגילה (6 אותיות)

6 מאונך: קודפתוח תוכנת יישום לקוח הנגישה לציבור ושנבדקה באופן עצמאי (7 אותיות)

מפתח פתרונות: מילים מבולבלות ופענוח הצופן

מפתח הערכה לפעילות פענוח מילות אוצר המילים ולאתגר הצופן הסודי.

מפתח פענוח מילים מבולבלות

1. בלהי — ליבה
2. תמנשרג — מגנרשת
3. התמפסהקג — מתגהפסקה
4. רדריאגווי — ווירגארד
5. ווההאס — הסוואה
6. ישיויחווזק — חוקישווייץ
7. קותחופד — קודפתוח
8. צקפו — צופן

מפתח אתגר הצופן הסודי

"שרתי ליבה מאובטחת מגנים על נתונים"

מפתח תשובות למקרי הבוחן

A מקרה בוחן 1: עקיפת חומות אש מגבילות

פתרון למורה

מחוון הערכה והנחיות לפתרון

- ניתוח תרחיש: משתמש נוסע למדינה שבה תעבורת VPN סטנדרטית כמו OpenVPN ו-WireGuard נחסמת על ידי DPI.
- שאלת מיקוד: איזו הגדרת פרוטוקול של Proton VPN מאפשרת למשתמש לעקוף בדיקה ברמת המדינה?
- אסטרטגיה ופתרון מומלצים: על המשתמש להפעיל את פרוטוקול Stealth, שמסווה את כותרות חבילות ה-VPN כתעבורת אינטרנט רגילה של TLS/HTTPS ועוקף מסנני DPI.

B מקרה בוחן 2: הגנה מפני יריבים מתקדמים

פתרון למורה

מחוון הערכה והנחיות לפתרון

- ניתוח תרחיש: מבקר פיננסי חושד שצומת היציאה של ספק האינטרנט המקומי שלו עלול להיות מנוצל על ידי איומים מתמשכים מתקדמים.
- שאלת מיקוד: כיצד Secure Core מגן על זהות המבקר מפני פגיעה בצומת היציאה?
- אסטרטגיה ופתרון מומלצים: Secure Core מנתב תעבורה תחילה דרך שרתים בבעלות Proton בשווייץ, באיסלנד או בשוודיה, ולכן שרת יציאה שנפרץ לא יכול לאתר את ה-IP של המשתמש.