שם: _____ תאריך: _____ ציון: _____

VPN לגישה מרחוק

אבטחת נקודות קצה של כוח עבודה מרוחק, אימות רב-גורמי והגדרות מנהרות IPsec.

סקירת למידה: VPN לגישה מרחוק

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 רשתות VPN לגישה מרחוק. תחקרו מנהרות לקוח-לאתר, כניסות רב-גורמיות, בדיקות מצב נקודות קצה, מגבלות רוחב פס וביקורת אבטחה באמצעות syslog.

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/best-vpn-for-business/remote-access/

מפת הלמידה שלכם: VPN לגישה מרחוק

- אבטחת נקודות קצה של כוח עבודה מרוחק הניגשות לצמתי רשת מקומיים.
- הגדירו מדיניות אימות רב-שלבי לכניסות מרחוק.
- הגדרת תצורות IPsec ו-OpenVPN מסוג client-to-site.
- בדקו יומני חיבור מרחוק לאיתור הפרות של בקרת גישה.
- יישמו בדיקות מצב מכשיר לפני מתן קישורי רשת.
- בצעו אופטימיזציה של תפוקת השרת כדי למנוע חנק של רוחב הפס בעבודה מרחוק.

הוראות VPN לגישה מרחוק

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 בדיקות מצב המכשיר (posture checks) והתחברות מרובת גורמים. ולסיום, פעילות הבונוס "חשבו מהר".

מנהרות לקוח-לאתר ועמידה בדרישות בנקודות קצה (מבוא)

VPN לגישה מרחוק מקים מנהרות מאובטחות בין לקוח לאתר עבור עובדים מחוץ למשרד. אבטחת החיבורים האלה מחייבת אכיפת התחברות עם אימות רב-שלבי (MFA), ביצוע בדיקות תאימות מצב נקודת קצה וביקורת יומנים באמצעות אוספי syslog מרכזיים.

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

נקודת ביקורת 1: אתגר שאלות אמריקאיות

1. איזה תקן אימות כדאי שפורטלי VPN לגישה מרחוק יחייבו?

- A) רב-גורמי
- B) גורם יחיד
- C) לא מוצפן
- D) אורח מקומי

2. איזה פרוטוקול הוא התקן לאבטחת חיבורי לקוח-לאתר בעבודה מרחוק?

- A) OpenVPN
- B) SOCKS5
- C) PPTP
- D) FTP

3. איזו בדיקה מוודאת שמחשב נייד מרוחק נקי לפני ההתחברות?

- A) בדיקת מצב אבטחה (Posture check)
- B) בדיקת מהירות
- C) בדיקת ping
- D) ספירת זיכרון

4. היכן מאוחסנים יומני חיבורים של עובדים מרחוק לצורכי ביקורת אבטחה?

- A) שרת Syslog
- B) מפתח רישום
- C) זיכרון הלקוח
- D) דפדפן אינטרנט

5. איזו בעיה מתרחשת כשמספר העובדים מרחוק עולה על קיבולת רוחב הפס של השער?

- A) חנק של רוחב פס
- B) דליפת DNS
- C) אישור לחיצת יד
- D) חשיפת IP

נקודת ביקורת 2: אתגר נכון או לא נכון

6 שאלה 6

6. אימות רב-גורמי מוסיף אסימון אימות משני כדי לאבטח התחברויות מרחוק.

נכון לא נכון

7 שאלה 7

7. בדיקות מצב אבטחה מאפשרות למכשירים מרוחקים עם חומות אש מושבתות לגשת לשרתים פרטיים.

נכון לא נכון

8 שאלה 8

8. יומני VPN לגישה מרחוק חיוניים לאיתור כניסה לא מורשית לרשת הארגונית.

נכון לא נכון

9 שאלה 9

9. OpenVPN ו-IPsec הם פרוטוקולים מיושנים שאינם מצליחים להצפין את תוכן הלקוחות מרחוק.

נכון לא נכון

10 שאלה 10

10. צוואר בקבוק ברוחב הפס של השער מתרחש כאשר התעבורה מרחוק חורגת מיכולת כרטיס החיבור.

נכון לא נכון

נקודת ביקורת 3: השלמת מונחי מפתח

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

1. כדי להגן על פורטלים ארגוניים, כניסות מרחוק חייבות לדרוש אימות _____ .
2. לקוחות מרחוק מצפינים את מטען המנהרה באמצעות פרוטוקולים סטנדרטיים כגון _____ .
3. מכשירים חייבים לעבור בדיקת _____ אבטחה לפני קבלת חיבורי רשת.
4. יומני כניסה הניתנים לביקורת מועברים באופן רציף לשרת _____ מרכזי.
5. תעבורה כבדה בשעות העבודה עלולה לגרום לעומס בשער עקב מגבלת _____ .
6. מנהלי התקנים של מתאם וירטואלי אחראים על _____ מסוג לקוח-אתר ב-Windows וב-macOS.

בנק מילים

הצפנה | חומת אש | מנהור | רב גורמי | רוחב פס | תקינות | OpenVPN | Syslog

כתבו את תשובותיכם כאן:

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

נקודת ביקורת 4: התאמת מושגי מפתח

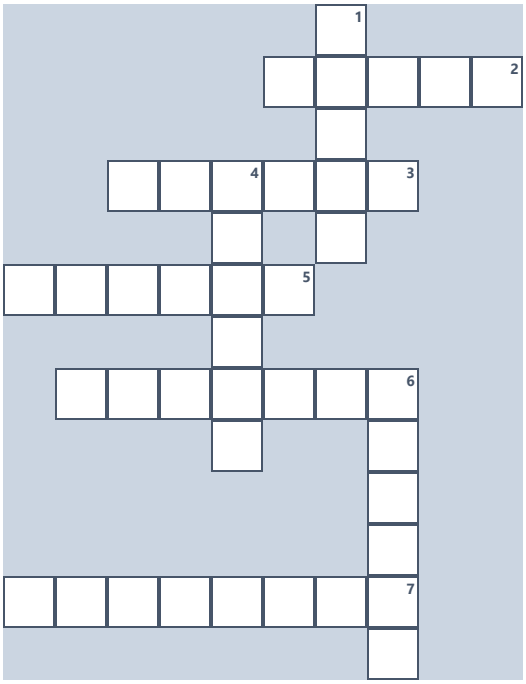
התאמת הגדרות

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

1. רב-גורמי	A	עטיפת נתונים בנתיב מאובטח.
2. OPENVPN	B	אוסף מרכזי של יומני אבטחה.
3. מצב אבטחה	C	מגבלת קיבולת נתוני הרשת.
4. SYSLOG	D	פרוטוקול client-to-site סטנדרטי.
5. רוחב פס	E	אימות תקינות המכשיר מרחוק.
6. הצפנה	F	כללי מערכת סינון תעבורה.
7. מנהור	G	ערבול קריפטוגרפי של חבילות.
8. חומת אש	H	אבטחת התחברות הדורשת אסימונים נוספים.

נקודת ביקורת 5: תשבץ

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



מאוזן

2. ערבול קריפטוגרפי של חבילות (5)

3. כללי מערכת לסינון תעבורה (6)

5. אוסף מרכזי של יומני אבטחה (6)

6. אבטחת כניסה שמחייבת אסימונים נוספים (7)

7. תקן מקובל לחיבור בין לקוח לאתר (8)

מאונך

1. הכלת נתונים בנתיב מאובטח (5)

4. אימות מצבו של מכשיר מרוחק (6)

6. מגבלת קיבולת הנתונים ברשת (6)

נקודת ביקורת 5 – פעילות חלופית: רמזים נגישים לתשבץ

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

מאוזן

2 מאוזן: ערבול קריפטוגרפי של חבילות (5 אותיות):

3 מאוזן: כללי מערכת לסינון תעבורה (6 אותיות):

5 מאוזן: אוסף מרכזי של יומני אבטחה (6 אותיות):

6 מאוזן: אבטחת כניסה שמחייבת אסימונים נוספים (7 אותיות):

7 מאוזן: תקן מקובל לחיבור בין לקוח לאתר (8 אותיות):

מאונך

1 מאונך: הכלת נתונים בנתיב מאובטח (5 אותיות):

4 מאונך: אימות מצבו של מכשיר מרוחק (6 אותיות):

6 מאונך: מגבלת קיבולת הנתונים ברשת (6 אותיות):

נקודת ביקורת 6: חיפוש מילה נסתרת

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

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

רשימת מילים

רבגורמי | פרוטוקול | תקינות | סיסלוג | רוחבפס | הצפנה | מנהור | חומתאש

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. רבגורמי
B. פרוטוקול
C. תקינות
D. סיסלוג
E. רוחבפס
F. הצפנה
G. מנהור
H. חומתאש

הגדרות ושדות התאמה	
1. אוסף מרכזי של יומני אבטחה.	
2. כללי מערכת לסינון תעבורה.	
3. הכלת נתונים בנתיב מאובטח.	
4. ערבול קריפטוגרפי של חבילות.	
5. תקן מקובל לחיבור בין לקוח לאתר.	
6. מגבלת קיבולת הנתונים ברשת.	
7. אימות מצבו של מכשיר מרוחק.	
8. אבטחת כניסה שמחייבת אסימונים נוספים.	

נקודת ביקורת 7: אתגר מילים מבולבלות

סדרו מחדש את האותיות שלהלן כדי לחשוף את המושגים המרכזיים בדף עבודה זה. כתבו את תשובותיכם בתיבות הקלט המסופקות.

1. ומרריגב
2. תתיונק
3. רחבספו
4. הרומנ
5. וקרלטפוו
6. ולססגי
7. נההפצ
8. משחאתו

פעילות בונוס: חשבו מהר

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

1	מיתוסים על VPN		
2	מילים שמתארות Zero Trust		
3	תוכנות משרדיות שאתם מכירים		
4	כללים לעבודה מרחוק בטוחה		
5	דברים שספק האינטרנט שלכם יכול לראות		
6	שירותי VPN שאתם מכירים		
7	מקומות שעובדים עובדים מהם		
8	כלים שחברה משתמשת בהם בכל יום		
9	תפקידים במחלקת IT		
10	מכשירים שיכולים להיות לעובד		
11	נתונים שחברה חייבת להגן עליהם		
12	דברים שעושים אחרי פריצת אבטחה		
13	דברים שעלולים לשבש פגישת וידאו		
14	דרכים להתחבר בצורה מאובטחת		
15	סיבות להעניק לעובדים VPN		

נקודת ביקורת 8: מקרי בוחן ב-VPN וברשתות

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

מקרה בוחן 1: אכיפת MFA

👨‍💻

תרחיש: אנליסט עסקי מנסה להתחבר למסד הנתונים של החברה בעבודה מרחוק. הוא מזין שם משתמש וסיסמה נכונים, אך פורטל ה-VPN חוסם את הגישה ודורש קוד מאסימון פיזי.

שאלה לדיון: איזו מדיניות אבטחה אוכפת את שלב האימות הכפול הזה?

מקרה בוחן 2: ציות למצב אבטחה

👨‍💻

תרחיש: קבלן מחבר את המחשב הנייד האישי שלו לרשת החברה מרחוק. לקוח ה-VPN מנתק מיד את החיבור ומודיע למשתמש שהגדרות הווירוסים באנטי-וירוס שלו אינן מעודכנות.

שאלה לדיון: איזו בדיקה ייעודית של שער ה-VPN חסמה את ניסיון ההתחברות הזה?

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	3	13		19	6	8	20	13		5	21	10	3

22	6	10	14	6	3	20	1		22	6	14	8	22

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 VPN לגישה מרחוק?

שיטת חיבור מאובטחת שמאפשרת לעובדים בעבודה מחוץ למשרד להתחבר ישירות לשרתים ארגוניים פרטיים.

Q2: במה שונה לקוח-לאתר מאתר-לאתר?

Client-to-site מחבר מכשירי משתמשים בודדים, ואילו Site-to-site מקשר בין אתרי משרדים פיזיים שלמים.

Q3: מהי בדיקת מצב מכשיר (device posture check)?

סריקה שבודקת את מצב האבטחה של מכשיר מרוחק (אנטי-וירוס, רמת עדכוני מערכת ההפעלה) לפני מתן גישה.

Q4: מדוע OpenVPN משמש לגישה מרחוק?

בשל פרוטוקול האבטחה החזק שלה, התאימות בין פלטפורמות והיכולת לטפל בחיבורים בודדים.

Q5: כיצד MFA מגן על גישה מרחוק?

הוא מוסיף אסימון אימות משני ומונע גישה גם אם סיסמאות העובדים דלפו או נגנבו.

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

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

Q6: מהו שרת syslog?

מאגר יומנים מרכזי שמאחסן אירועי חיבור, התחברויות והתראות מערכת לצורכי ביקורות עמידה בדרישות.

Q7: מה גורם לחנק של רוחב פס?

כשדרישות רוחב הפס המצטברות של עובדים מרחוק חורגות ממגבלת מהירות האינטרנט של שער הארגון.

Q8: האם אפשר לחבר את המחשב הביתי שלי ל-VPN של העבודה?

רק אם המכשיר עובר בדיקות ביקורת מצב אבטחה של החברה ומאושר על ידי מנהלי ה-IT.

Q9: מהי אנקפסולציה ברשת?

עטיפת מנות נתונים במעבר בתוך כותרות פרוטוקול מוצפנות כדי לאבטח את השידור.

Q10: כיצד פיצול מנהרה מייעל גישה מרחוק?

הוא מאפשר לעובדים להשתמש בספק האינטרנט המקומי שלהם לגלישה רגילה ולנתב קבצים הקשורים לעבודה דרך ה-VPN.

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 אימות מבוסס אישורים משפר גישה מרחוק?

הוא קושר הרשאות חיבור לאישורים דיגיטליים מקומיים שהותקנו מראש וחוסם מכשירים שאינם מנוהלים או מורשים.

Q2: מהו הסיכון האבטחתי של פיצול מנהרה בעבודה מרחוק?

הוא יוצר גשר פוטנציאלי שדרכו מכשיר מקומי שנפרץ יכול לנתב איומים חיצוניים לרשת הפרטית.

Q3: כיצד בדיקות מצב (posture checks) בוחנות הגדרות רישום?

לקוח ה-VPN מריץ סקריפטים מקומיים ששואלים נתיבי רישום (registry) כדי לוודא אם תוכנת אבטחה ארגונית פועלת.

Q4: מדוע syslog משתמש כברירת מחדל בפורט UDP 514?

כדי להעביר יומנים במהירות עם תקורה מינימלית, אם כי הגדרות מאובטחות מחייבות כיום עטיפת TLS מעל TCP.

Q5: כיצד חברות פותרות צווארי בקבוק ברוחב הפס של השער?

על ידי יישום מאזני עומסים וחלוקת תעבורה מרוחקת בין צמתי שרתים אזוריים.

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

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

Q6: מה תפקידם של מתאמי TAP/TUN וירטואליים בלקוחות מרוחקים?

הם משמשים ככרטיסי רשת וירטואליים ומנתבים תעבורת TCP/IP ברמת המכשיר ישירות אל מנהרת ה-VPN המוצפנת.

Q7: כיצד IKEv2 MOBIKE תומך בניידות של כוח עבודה מרוחק?

הוא מעדכן באופן דינמי קישורי כתובות IP ושומר על ה-VPN פעיל בזמן שהמשתמש עובר בין Wi-Fi לנתונים סלולריים.

Q8: מה ההבדל בין ניתוב מפוצל לניתוב במנהרה מלאה?

ניתוב מלא מכריח את כל תעבורת האינטרנט של המכשיר לעבור דרך ה-VPN, ואילו ניתוב מפוצל שולח רק כתובות IP של יעדים ארגוניים.

Q9: כיצד התקני NAT מטפלים בחיבורי VPN מרוחקים?

על ידי מיפוי טווחי פורטים מקומיים לכתובות IP של שער ציבורי כדי לנתב חבילות נתונים מוצפנות חוזרות.

Q10: אילו תקני ציות מחייבים ביקורת גישה מרחוק?

תקנים כמו HIPAA, SOC 2 ו-PCI DSS דורשים תיעוד וניטור של כל סשני החיבור מרחוק.

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

VPN לגישה מרחוק מקים מנהרות מאובטחות בין לקוח לאתר עבור עובדים מחוץ למשרד.

2. תובנות על VPN

כללי ציות מחייבים אימות רב-גורמי כדי להגן על פורטלים עסקיים מרוחקים.

3. תובנות על VPN

בדיקות מצב אבטחה מאמתות את הגדרות האבטחה המקומיות של הלקוח לפני מתן גישה לרשת פרטית.

4. תובנות על VPN

שרתי Syslog מרכזים יומני חיבור לצורך ביקורת וזיהוי ניסיונות גישה לא מורשים.

5. תובנות על VPN

צווארי בקבוק ברוחב הפס של השער מתרחשים כאשר הביקוש המצטבר לתעבורה מרחוק חורג ממגבלות האינטרנט של השרת.

6. תובנות על VPN

מתאמי רשת וירטואליים עוטפים שאילתות רשת של מערכת ההפעלה בתוך פרוטוקולים מאובטחים.

7. תובנה על VPN

תמיכה ב-MOBIKE מאפשרת ללקוחות מרוחקים להחליף רשתות מבלי לנתק את מנהרת ה-VPN.

8. תובנה על VPN

ניתוב מנהרה מלאה מאבטח את כל תעבורת האינטרנט של העובדים אך מגדיל את העומס על שער הארגון.

9. תובנה על VPN

אימות באמצעות תעודה קושר את ההרשאה לחיבור VPN ישירות לחומרה המנוהלת על ידי החברה.

10. תובנות על VPN

מסגרות כמו SOC 2 ו-PCI DSS מצפות לתיעוד וניטור של מפגשי גישה מרחוק.

מקורות והפניות טכניים

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

מקורות אקדמיים ותעשייתיים

[1] VPN.com. (2026). Best VPN for Business: Tested & Ranked By Our Experts.
https://www.vpn.com/vpn/best-vpn-for-business/

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

[3] NIST. (2016). SP 800-46 Rev. 2: Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security.
https://csrc.nist.gov/pubs/sp/800/46/r2/final

[4] NordLayer. (n.d.). Secure your network & stay compliant with one toggle-ready platform.
https://nordlayer.com/

[5] IETF. (2006). RFC 4555: IKEv2 Mobility and Multihoming Protocol (MOBIKE).
https://www.rfc-editor.org/rfc/rfc4555

מפתח תשובות: נקודת ביקורת 1 – שאלות אמריקאיות

1 **אסימוני התחברות** אבטחת MFA

תשובה נכונה: A

הערה למורה

אימות רב-גורמי אוכף אימות משני להתחברויות. ציטוט: MFA Implementation.

2 **מנהרת OpenVPN** לקוח-לאתר

תשובה נכונה: A

הערה למורה

OpenVPN הוא פרוטוקול סטנדרטי לאבטחת מנהרות בין לקוח לאתר. מקור: OpenVPN Client.

3 **ביקורות מצב אבטחה** בדיקת מכשיר

תשובה נכונה: A

הערה למורה

בדיקות מצב אבטחה סורקות נקודות קצה לאיתור חומות אש וכלי אנטי-וירוס פעילים. מקור: Posture Compliance.

4 **מקבץ יומנים** שרת SYSLOG

תשובה נכונה: A

הערה למורה

שרתי Syslog אוספים יומני אירועי אבטחה לניטור הפרות גישה. מקור: Syslog Standard.

5 **גלישת כרטיסים** צוואר בקבוק בשער

תשובה נכונה: A

הערה למורה

צוואר בקבוק ברוחב הפס של השער מתרחש כאשר תעבורת המשתמשים חורגת ממגבלות השרת. מקור: Capacity Planning.

מפתח תשובות: נקודת ביקורת 2 – נכון או לא נכון

6 **אסימוני התחברות** בדיקות MFA

תשובה נכונה: נכון

הערה למורה

אימות רב-גורמי אוכף אימות משני להתחברויות. ציטוט: MFA Implementation.

7 **שאלה 7**

תשובה נכונה: לא נכון

הערה למורה

בדיקות מצב (posture checks) חוסמות מכשירים שחומת האש או האנטי-וירוס שלהם כבויים, ולכן מכשירים כאלה נדחים.

8 **מקבץ יומנים** שרת SYSLOG

תשובה נכונה: נכון

הערה למורה

שרתי Syslog אוספים יומני אירועי אבטחה לניטור הפרות גישה. מקור: Syslog Standard.

9 **שאלה 9**

תשובה נכונה: לא נכון

הערה למורה

OpenVPN ו-IPsec הם פרוטוקולים עדכניים שאכן מצפינים תעבורת לקוחות מרוחקים.

10 **גלישת כרטיסים** צוואר בקבוק בשער

תשובה נכונה: נכון

הערה למורה

צוואר בקבוק ברוחב הפס של השער מתרחש כאשר תעבורת המשתמשים חורגת ממגבלות השרת. מקור: Capacity Planning.

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. רב-גורמי	D 2. OPENVPN	E 3. מצב אבטחה	B 4. SYSLOG
C 5. רוחב פס	G 6. הצפנה	A 7. מנהור	F 8. חומת אש

נקודת ביקורת 3: מפתח תשובות – מונחי מפתח

1 רב גורמי	2 OpenVPN	3 תקינות	4 Syslog
5 רוחב פס	6 מנהור		

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

1 D – סיסלוג	2 H – חומתאש	3 G – מנהור	4 F – הצפנה
5 B – פרוטוקול	6 E – רוחבפס	7 C – תקינות	8 A – רבגורמי

הערות לדיון עבור מורים

מונחי מפתח:
ודאו שהתלמידים מסבירים במילים שלהם את רב-גורמי, OPENVPN ו-מצב אבטחה ונותנים דוגמה לכל אחד מהם.

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

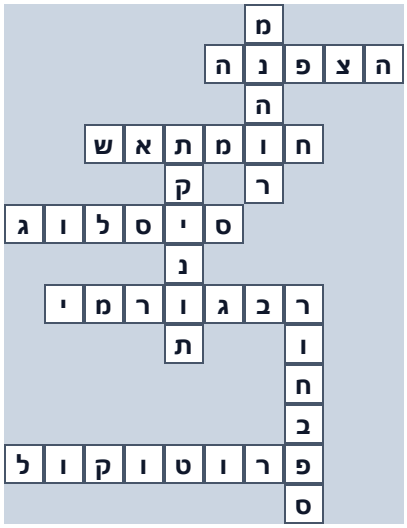
הערכת מקורות:
בקשו מהתלמידים לאמת לפחות טענה אחת במקורות של דף העבודה, ודונו מדוע נתונים, מחירים וכללים עשויים להשתנות עם הזמן.

מפתחות פאזלים והערות למורה

פתרון תפזורת

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

פתרון תשבץ



מדריך למורה לפתרונות התשבץ

מאוזן

2 מאוזן: הצפנה ערבול קריפטוגרפי של חבילות (5 אותיות)

3 מאוזן: חומתאש כללי מערכת לסינון תעבורה (6 אותיות)

5 מאוזן: סיסלוג אוסף מרכזי של יומני אבטחה (6 אותיות)

6 מאוזן: רבגורמי אבטחת כניסה שמחייבת אסימונים נוספים (7 אותיות)

7 מאוזן: פרוטוקול תקן מקובל לחיבור בין לקוח לאתר (8 אותיות)

מאונך

1 מאונך: מנהור הכלת נתונים בנתיב מאובטח (5 אותיות)

4 מאונך: תקינות אימות מצבו של מכשיר מרוחק (6 אותיות)

6 מאונך: רוחבפס מגבלת קיבולת הנתונים ברשת (6 אותיות)

מפתח פתרונות: מילים מבולבלות ופענוח הצופן

מפתח הערכה לפעילות פענוח מילות אוצר המילים ולאתגר הצופן הסודי.

מפתח פענוח מילים מבולבלות

1. ומרריגב — רבגורמי
2. תתיונק — תקינות
3. רחבספו — רוחבפס
4. הרומנ — מנהור
5. וקרלטפוו — פרוטוקול
6. ולססגי — סיסלוג
7. נההפצ — הצפנה
8. משחאתו — חומתאש

מפתח אתגר הצופן הסודי

"גישה מרחוק מגנה על תחנות ארגוניות"

מפתח תשובות למקרי הבוחן

A מקרה בוחן 1: אכיפת MFA

פתרון למורה

הנחיות הערכה

תשובות התלמידים צריכות לכלול את הנקודות הבאות:

- ניתוח תרחיש: אנליסט עסקי מנסה להתחבר למסד הנתונים הארגוני שלו בעבודה מרחוק. הוא מזין שם משתמש וסיסמה נכונים, אך פורטל ה-VPN חוסם את הגישה ודורש קוד אסימון פיזי.
- אסטרטגיה ופתרון מומלצים: פורטל ה-VPN הארגוני אוכף מדיניות אימות רב-שלבי (MFA) מחמירה כדי לאבטח התחברויות מרחוק.

B מקרה בוחן 2: ציות למצב אבטחה

פתרון למורה

הנחיות הערכה

תשובות התלמידים צריכות לכלול את הנקודות הבאות:

- ניתוח תרחיש: קבלן מחבר את המחשב הנייד האישי שלו לרשת הארגונית מרחוק. לקוח ה-VPN מנתק מיד את החיבור ומודיע למשתמש שהגדרות האנטי-וירוס שלו אינן מעודכנות.
- אסטרטגיה ופתרון מומלצים: שער הגישה מרחוק ביצע בדיקת מצב נקודת קצה (endpoint posture) וחסם את המכשיר בגלל הגדרות אבטחה לא מעודכנות.