שם: _____ תאריך: _____ ציון: _____

VPN ארגוני

הטמעת גישה לרשת בגישת Zero Trust, צמתי שער ייעודיים ובקרות ניהול ארגוניות מרכזיות.

סקירת למידה: רשתות VPN ארגוניות

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 ארגוניות. תחקרו ארכיטקטורות Zero Trust, שערי IP סטטיים ייעודיים, קונסולות ניהול, הקצאת משתמשים ומנהרות IPsec בין אתרים.

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/enterprise/

מפת הלמידה שלכם: רשת VPN ארגונית

- יישמו מסגרות גישה לרשת בגישת Zero Trust (ZTNA).
- הגדירו כתובות IP ייעודיות של שערי שרתים עבור מסנני רשימה לבנה.
- ניהול לוחות ניהול ארגוניים מרכזיים ורשימות מושבי משתמשים.
- בדקו יומני גישה לרשת והיסטוריות חיבור של משתמשים.
- הגדירו כללי כניסה יחידה (SSO) ואימות רב-שלבי.
- הקמת מנהרות IPsec מסוג site-to-site בין סניפים.

הוראות לרשתות VPN ארגוניות

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 Zero Trust ו-IPsec בין אתרים (site-to-site). ולסיום, פעילות הבונוס "חשבו מהר".

ארכיטקטורות Zero Trust ושערים ייעודיים (מבוא)

רשתות VPN ארגוניות מאבטחות נכסים ארגוניים באמצעות מעבר למסגרות Zero Trust Network Access (ZTNA) והוספה לרשימה מותרת של שערי IP סטטיים ייעודיים. מנהלי IT משתמשים בקונסולות ניהול מרכזיות כדי לתזמר מנהרות IPsec מסוג אתר-לאתר וקישורי כניסה יחידה (SSO).

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

נקודת ביקורת 1: אתגר שאלות אמריקאיות

1. איזה מודל אבטחה מחליף VPN ארגוניים ישנים?

- A) Zero Trust
- B) Multi-hop
- C) עמית-לעמית (Peer-to-peer)
- D) שער יחיד

2. איזו תכונה נדרשת כדי להגביל גישה למסד נתונים לשרתי החברה?

- A) IP ייעודי
- B) ניתוב דינמי
- C) פיצול מנהרה
- D) proxy של DNS

3. איזה פרוטוקול הוא התקן למנהרות אתר-לאתר ארגוניות?

- A) IPsec
- B) PPTP
- C) SOCKS5
- D) SSL v3

4. איזה כלי מרכזי מאפשר למנהלים לנהל מושבי עובדים?

- A) קונסולת ניהול
- B) מפתח רישום
- C) קושחת נתב
- D) יומן מערכת

5. איזה תקן אימות מאפשר התחברות דרך Okta או Microsoft Entra ID?

- A) כניסה יחידה (Single Sign-On)
- B) סוד משותף
- C) אימות EPP
- D) מפתח WEP

נקודת ביקורת 2: אתגר נכון או לא נכון

שאלה 6

6. Zero Trust Network Access מעניק כניסה לרשת רק לאחר אימות מתמשך של אמון המכשיר.

נכון ○ לא נכון ○

שאלה 7

7. שערי IP ייעודיים מנתבים את תעבורת העובדים לצד משתמשים ציבוריים אקראיים.

נכון ○ לא נכון ○

שאלה 8

8. קונסולות ניהול מרכזיות מאפשרות למנהלי IT לבטל באופן מיידי מושבים של עובדים בודדים.

נכון ○ לא נכון ○

שאלה 9

9. IPsec הוא פרוטוקול קל משקל שאינו תומך במנהרות רשת בין אתרים (site-to-site).

נכון ○ לא נכון ○

שאלה 10

10. Single Sign-On מאפשר אימות מאובטח של עובדים באמצעות ספקי זהות ארגוניים.

נכון ○ לא נכון ○

נקודת ביקורת 3: השלמת מונחי מפתח

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

1. ארכיטקטורות אבטחה מודרניות מחליפות מנהרות ישנות בגישת _____ .
2. כדי להגביל גישה למסד נתונים, חברות מגדירות כתובת שער עם IP _____ .
3. סניפים מחוברים בצורה מאובטחת באמצעות מנהרות _____ בין אתרים.
4. מנהלי IT מקצים רישיונות משתמש לעובדים בממשק ניהול מרכזי הנקרא _____ .
5. שילוב עם Okta מאפשר לעובדים להזדהות באמצעות _____ ארגונית.
6. כדי להגן על הכניסות, פורטלים ארגוניים מחייבים אימות _____ .

בנק מילים

אפס אמון | הקצאה | ייעודי | כניסה אחת | קונסולת ניהול | רב גורמי | שער | IPsec

כתבו את תשובותיכם כאן:

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

נקודת ביקורת 4: התאמת מושגי מפתח

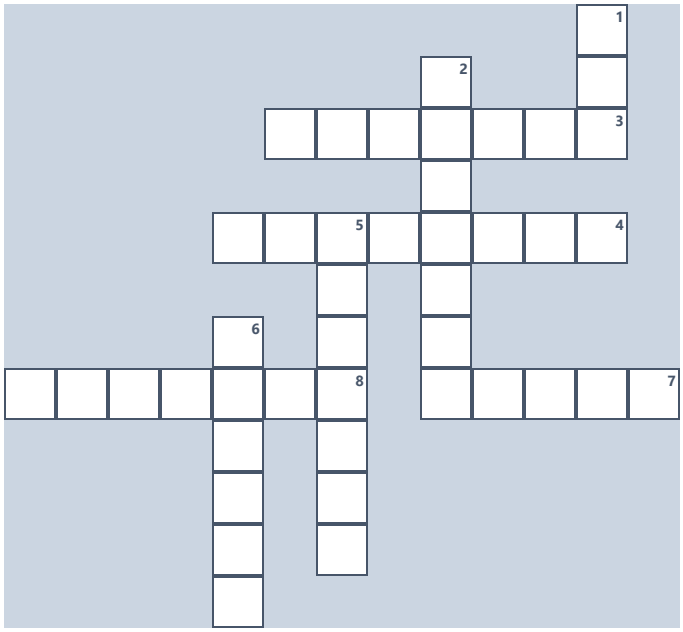
התאמת הגדרות

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

1. אפס אמון	A	הקצאת רישיונות גישה ל-VPN לעובדים.
2. כתובת IP ייעודית	B	הקישור בין זהויות של Okta ו-Entra ID.
3. IPSEC	C	אבטחת התחברות הדורשת אסימונים נוספים.
4. קונסולת ניהול	D	כתובת שער ברשימת היתרים סטטית.
5. כניסה יחידה	E	תקן מנהרות site-to-site.
6. רב-גורמי	F	צומת ניתוב כניסה לרשת.
7. שער	G	פורטל מרכזי של מנהל IT לניהול מושבים.
8. הקצאה	H	מסגרת לאימות אמון רציף.

נקודת ביקורת 5: תשבץ

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



מאוזן

3. אבטחת כניסה שמחייבת אסימונים נוספים (7)

4. קישור זהויות עם Okta ו-Entra ID (8)

7. חלוקת רישיונות גישת VPN לעובדים (5)

8. תקן מנהרה בין אתרים (7)

מאונך

1. צומת ניתוב בכניסה לרשת (3)

2. פורטל מרכזי שבו מנהלי ה-IT מנהלים את המושבים (7)

5. מסגרת לאימות אמון מתמשך (7)

6. כתובת שער סטטית לרשימה הלבנה (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: אבטחת כניסה שמחייבת אסימונים נוספים (7 אותיות):

4 מאוזן: קישור זהויות עם Okta ו-Entra ID (8 אותיות):

7 מאוזן: חלוקת רישיונות גישת VPN לעובדים (5 אותיות):

8 מאוזן: תקן מנהרה בין אתרים (7 אותיות):

מאונך

1 מאונך: צומת ניתוב בכניסה לרשת (3 אותיות):

2 מאונך: פורטל מרכזי שבו מנהלי ה-IT מנהלים את המושבים (7 אותיות):

5 מאונך: מסגרת לאימות אמון מתמשך (7 אותיות):

6 מאונך: כתובת שער סטטית לרשימה הלבנה (6 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	ק	ד	ח	ל	ל	י	ס
נ	ז	ל	ל	ס	ע	פ	צ	צ	ו	ו	ב	פ	ס	מ
ח	ע	י	מ	ר	ו	ג	ב	ר	ב	נ	ר	ד	פ	ן
ק	ג	ן	ר	ו	כ	י	ז	י	ן	ד	ס	ל	ד	ע
ק	ש	נ	ב	ק	נ	ב	א	א	ד	ן	מ	ו	ד	י
ס	ר	א	ד	מ	י	ד	ה	פ	ז	ו	ח	ד	ל	ע
י	ע	ס	ל	ה	ס	ח	ע	ן	ס	פ	ע	ה	ע	ה
פ	ש	ר	ה	א	ה	א	ע	נ	ל	א	נ	י	צ	ש
י	ס	ט	ע	צ	א	ה	פ	ג	ל	ת	מ	ב	י	ו
י	ע	ש	ש	ט	ח	ק	א	ע	ן	ת	ת	ו	כ	ו
א	ח	ל	ע	ט	ת	צ	כ	כ	צ	נ	ז	ס	ן	ס
ז	ן	א	מ	ק	ו	א	ק	ב	ת	ע	ת	ב	ז	כ
ן	ו	ט	מ	נ	מ	ה	ש	ג	כ	ן	ת	ו	ת	נ
ר	ק	י	ק	נ	ב	מ	ר	צ	כ	ז	ק	ג	ת	ק

רשימת מילים

אפסאמון | ייעודי | אייפיסק | קונסולה | כניסהאחת | רבגורמי | שער | הקצאה

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	הגדרות ושדות התאמה
A. אפסאמון	1. כתובת שער סטטית לרשימה הלבנה. ____
B. ייעודי	2. צומת ניתוב בכניסה לרשת. ____
C. אייפיסק	3. חלוקת רישיונות גישת VPN לעובדים. ____
D. קונסולה	4. אבטחת כניסה שמחייבת אסימונים נוספים. ____
E. כניסהאחת	5. תקן מנהרה בין אתרים. ____
F. רבגורמי	6. מסגרת לאימות אמון מתמשך. ____
G. שער	7. קישור זהויות עם Okta ו-Entra ID. ____
H. הקצאה	8. פורטל מרכזי שבו מנהלי ה-IT מנהלים את המושבים. ____

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. אואמןספ
2. איקסיפי
3. סנכהאתחי
4. ערש
5. ועיידי
6. לנוקסהו
7. רמריבוג
8. ההצאק

פעילות בונוס: חשבו מהר

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

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

נקודת ביקורת 8: מקרי בוחן ב-VPN וברשתות

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

מקרה בוחן 1: מעבר ל-Zero Trust

👨‍💻

תרחיש: ארגון רוצה לאבטח את השרתים המקומיים שלו על ידי אימות מתמשך של אישורי תאימות המכשירים, מצב חומת האש ומיקום המשתמש, במקום לתת אמון בכל מי שנמצא בתוך הרשת.

שאלה לדיון: באיזה מסגרת עבודה על מנהל אבטחת ה-IT ליישם כדי להשיג זאת?

מקרה בוחן 2: הגבלת שער

👨‍💻

תרחיש: חברה מארחת מסדי נתונים פיננסיים פרטיים בענן. היא רוצה לחסום כל גישה מהאינטרנט הציבורי ללוחות הניהול, ולאפשר התחברות רק מתחנות קצה מאומתות של החברה.

שאלה לדיון: איזו תצורת רשת על מנהל מסד הנתונים להגדיר בחומת האש בענן?

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

20	10	21	11	13	12	11	22	13	1	13	25	6	13	1	15	17	1		
							22	21	20	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 על רשתות פרטיות וירטואליות (VPN) ועל מנהור.

Q1: מהו VPN ארגוני?

מנהרת רשת מאובטחת שנועדה לעסקים, ומאפשרת לעובדים מרחוק לגשת לרשתות ארגוניות עם ניהול מרכזי.

Q2: במה Zero Trust שונה מ-VPN מסורתיים?

ב-VPN מסורתי סומכים על כל מי שבתוך המנהרה, ואילו Zero Trust מאמת ברציפות כל מכשיר וכל חיבור משתמש.

Q3: מהי כתובת IP ייעודית ב-VPN עסקי?

כתובת IP סטטית השמורה אך ורק לעסק שלך, ומאפשרת להוסיף אותה לרשימת היתרים לגישה מאובטחת למסדי נתונים בענן.

Q4: מדוע SSO חשוב ל-VPN עסקי?

Single Sign-On מאפשר לעובדים להשתמש בפרטי הגישה הארגוניים שלהם (כמו Okta או Microsoft Entra ID) כדי להתחבר בצורה מאובטחת.

Q5: מהו VPN מאתר לאתר?

מנהרה שמחברת שני משרדים פיזיים (כמו סניף ומטה) דרך האינטרנט הציבורי באמצעות IPsec.

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

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

Q6: מה תפקיד קונסולת הניהול?

לוח בקרה למנהלי IT להוספה או להסרה של מושבי עובדים, להקצאת שערים ולניטור חיבורים פעילים.

Q7: כיצד MFA מאבטח VPN עסקיים?

על ידי דרישת קוד משני (כמו אסימון מאפליקציית אימות) כדי למנוע כניסה לא מורשית באמצעות סיסמאות שנפרצו.

Q8: האם אפשר לבקר את היסטוריית החיבורים של עובדים?

כן, VPN ארגוניים רושמים חותמות זמן של חיבורים, משך וכתובות IP שהוקצו לצורכי ביקורת ציות.

Q9: מהו ZTNA?

Zero Trust Network Access, מודל אבטחה המעניק גישה רק ליישומים ספציפיים ולא לכל הרשת.

Q10: מהו תפקידם של צמתי שער?

הם משמשים נקודות כניסה מאובטחות לתעבורה מרוחקת ומנתבים נתונים ישירות לשרתים ארגוניים פרטיים.

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 IPsec מגן על תקשורת ארגונית בין אתרים?

IPsec מצפין תעבורה בשכבת הרשת באמצעות Encapsulating Security Payload (ESP) כדי להבטיח סודיות ושלמות של נתונים.

Q2: מדוע אבטחה מסורתית מבוססת היקף נכשלת עבור עובדים מרחוק?

מפני שעובדים ניגשים לנתונים ממספר מיקומים ומכשירים, מה שהופך היקף חומת אש יחיד של הרשת למיושן.

Q3: כיצד מנהלי IT מיישמים הקצאה אוטומטית?

על ידי מיפוי פרוטוקולי SCIM בין ספקי זהות (Okta) לקונסולת הניהול של ה-VPN לסנכרון ספריות משתמשים.

Q4: מה היתרון של split tunneling בסביבות ארגוניות?

הוא מנתב תעבורת SaaS מקומית (כמו Microsoft 365) מחוץ למנהרת ה-VPN ושומר את רוחב הפס של שער הארגון למסדי נתונים פרטיים.

Q5: כיצד בדיקות מצב מכשיר מאמתות את אבטחת נקודות הקצה?

לקוח ה-VPN סורק את המכשיר לפני החיבור כדי לוודא שחומת האש פעילה, האנטי-וירוס פועל ותיקוני מערכת ההפעלה מעודכנים.

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 תפקידו של מעבר NAT (NAT traversal) בהגדרות VPN עסקיות?

NAT-T עוטף חבילות IPsec ב-UDP כדי לאפשר להן לעבור דרך נתבים וחומות אש ביתיים ללא ניתוקי חיבור.

Q7: כיצד עסקים מונעים חנק של רוחב פס בשער?

על ידי פריסת מספר צמתי שער אזוריים ואיזון תעבורת המשתמשים הנכנסת ביניהם באמצעות מאזני עומסים.

Q8: מדוע רשימות היתר של IP סטטי מועדפות על פני דינמיות?

רשימות היתרים סטטיות מונעות מכתובות IP חיצוניות לא מורשות לנסות לבצע לחיצות יד לחיבור, ובכך מקטינות באופן דרמטי את משטח התקיפה.

Q9: מה תפקידו של אימות מבוסס אישורים ב-VPN ארגוניים?

הוא מאמת אישורים דיגיטליים ייחודיים המותקנים במכשירים בניהול החברה וחוסם מחשבים אישיים שאינם מנוהלים.

Q10: כיצד ZTNA מפחית את הסיכון לתנועה רוחבית?

על ידי בידוד סשנים של משתמשים למשאבים מורשים ספציפיים, מה שמונע מהאקרים לנוע ברשת אם צומת אחד נפרץ.

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

ארכיטקטורות Zero Trust מאמתות באופן מתמשך את מצב האבטחה של כל מכשיר המנסה להתחבר לרשת.

2. תובנות על VPN

שערי IP ייעודיים מאפשרים לעסקים לנעול מסדי נתונים בענן באמצעות הוספת כתובות סטטיות לרשימה מותרת.

3. תובנות על VPN

IPsec הוא פרוטוקול התקן בתעשייה להגדרת מנהרות מאובטחות בין רשתות משרדים (site-to-site).

4. תובנות על VPN

קונסולות ניהול מאפשרות למחלקות IT להקצות, לנהל ולבקר מושבי גישה של עובדים ל-VPN.

5. תובנות על VPN

Single Sign-On משלב גישת VPN עם ספקי זהות ארגוניים כמו Okta ו-Entra ID.

6. תובנות על VPN

אימות רב-גורמי חוסם ניסיונות חיבור לא מורשים שמקורם במפתחות סיסמה גנובים.

7. תובנה על VPN

Split tunneling מייעל את רוחב הפס הארגוני על ידי החרגת תעבורת SaaS ציבורית מהמנהרה המוצפנת.

8. תובנה על VPN

בדיקות מצב מכשיר מאמתות הגדרות אבטחה מקומיות לפני מתן גישה לשרתים ארגוניים.

9. תובנה על VPN

סנכרון ספריית SCIM מבצע אוטומציה של בקרות הגישה בקליטת עובדים ובעזיבתם.

10. תובנות על VPN

Zero Trust Network Access מגביל את גישת המשתמשים ליישומים מורשים ספציפיים ומונע תנועה רוחבית ברשת.

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/

מפתח תשובות: נקודת ביקורת 1 – שאלות אמריקאיות

1 **Zero Trust** מודל ZTNA **תשובה נכונה: A**

הערה למורה

מודלים של Zero Trust מאמתים באופן מתמשך את תאימות המכשיר לפני כניסה לרשת. ציטוט: NIST Zero Trust.

2 **כתובת IP ייעודית** IP סטטי **תשובה נכונה: A**

הערה למורה

כתובות IP ייעודיות מאפשרות להוסיף שערים לרשימה מותרת כדי לחסום תעבורה ציבורית. מקור: Dedicated IP Guide.

3 **תקן IPsec** מנהרת IPSEC **תשובה נכונה: A**

הערה למורה

IPsec הוא הפרוטוקול הסטנדרטי המשמש למנהרות site-to-site בין סניפים. מקור: IPsec Tunneling.

4 **הקצאת IT** קונסולת ניהול **תשובה נכונה: A**

הערה למורה

לוחות בקרה מנהליים מרכזיים מאפשרים למנהלי IT להקצות רישיונות מושבים. מקור: CISA Guidelines.

5 **שאלה 5** **תשובה נכונה: A**

הערה למורה

איזה תקן אימות מאפשר התחברות דרך Okta או Microsoft Entra ID? → כניסה יחידה (Single Sign-On)

מפתח תשובות: נקודת ביקורת 2 – נכון או לא נכון

6 **Zero Trust** — בדיקות ZTNA — **תשובה נכונה: נכון**

הערה למורה

מודלים של Zero Trust מאמתים באופן מתמשך את תאימות המכשיר לפני כניסה לרשת. ציטוט: NIST Zero Trust.

7 **שאלה 7** — **תשובה נכונה: לא נכון**

הערה למורה

כתובות IP ייעודיות שמורות לעסק אחד, כך שהתעבורה שלו אינה מעורבבת עם משתמשים אחרים.

8 **הקצאת IT** — עמדת מנהל IT — **תשובה נכונה: נכון**

הערה למורה

לוחות בקרה מנהליים מרכזיים מאפשרים למנהלי IT להקצות רישיונות מושבים. מקור: CISA Guidelines.

9 **תקן IPsec** — אתר לאתר — **תשובה נכונה: לא נכון**

הערה למורה

IPsec הוא הפרוטוקול הסטנדרטי המשמש למנהרות site-to-site בין סניפים. מקור: IPsec Tunneling.

10 **קישור SSO של Okta** — התחברות SSO — **תשובה נכונה: נכון**

הערה למורה

Single Sign-On משלב כניסות VPN עם ספריות ארגוניות כמו Okta. מקור: Okta SSO.

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. אפס אמון	D 2. כתובת IP ייעודית	E 3. IPSEC	G 4. קונסולת ניהול
B 5. כניסה יחידה	C 6. רב-גורמי	F 7. שער	A 8. הקצאה

נקודת ביקורת 3: מפתח תשובות – מונחי מפתח

1 אפס אמון	2 ייעודי	3 IPsec	4 קונסולת ניהול
5 כניסה אחת	6 רב גורמי		

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

1 B – ייעודי	2 G – שער	3 H – הקצאה	4 F – רבגורמי
5 C – אייפיסק	6 A – אפסאמון	7 E – כניסהאחת	8 D – קונסולה

הערות לדיון עבור מורים

מונחי מפתח:
ודאו שהתלמידים מסבירים במילים שלהם את אפס אמון, כתובת IP ייעודית ו-IPSEC ונותנים דוגמה לכל אחד מהם.

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

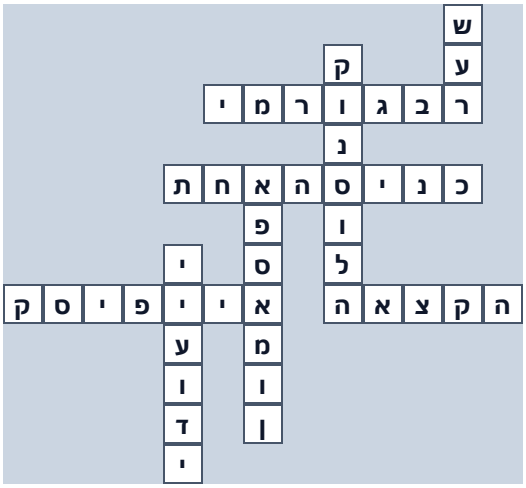
הערכת מקורות:
בקשו מהתלמידים לאמת לפחות טענה אחת במקורות של דף העבודה, ודונו מדוע נתונים, מחירים וכללים עשויים להשתנות עם הזמן.

מפתחות פאזלים והערות למורה

פתרון תפזורת

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

פתרון תשבץ



מדריך למורה לפתרונות התשבץ

מאוזן

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

4 מאוזן: כניסהאחת קישור זהויות עם Okta ו-Entra ID (8 אותיות)

7 מאוזן: הקצאה חלוקת רישיונות גישת VPN לעובדים (5 אותיות)

8 מאוזן: אייפיסק תקן מנהרה בין אתרים (7 אותיות)

מאונך

1 מאונך: שער צומת ניתוב בכניסה לרשת (3 אותיות)

2 מאונך: קונסולה פורטל מרכזי שבו מנהלי ה-IT מנהלים את המושבים (7 אותיות)

5 מאונך: אפסאמון מסגרת לאימות אמון מתמשך (7 אותיות)

6 מאונך: ייעודי כתובת שער סטטית לרשימה הלבנה (6 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. איקסיפי — אייפיסק
3. סנכהאתחי — כניסהאחת
4. ערש — שער
5. ועיידי — ייעודי
6. לנוקסהו — קונסולה
7. רמריבוג — רבגורמי
8. ההצאק — הקצאה

מפתח אתגר הצופן הסודי

"אפס אמון מאמת כל מכשיר לרשת"

מפתח תשובות למקרי הבוחן

A מקרה בוחן 1: מעבר ל-Zero Trust

פתרון למורה

הנחיות הערכה

תשובות התלמידים צריכות לכלול את הנקודות הבאות:

- ניתוח תרחיש: ארגון רוצה לאבטח את השרתים המקומיים שלו על ידי אימות מתמשך של אישורי תאימות המכשיר, מצב חומת האש ומיקום המשתמש, במקום לתת אמון בכל מי שנמצא בתוך הרשת.
- אסטרטגיה ופתרון מומלצים: על המנהל לעבור למודל Zero Trust Network Access (ZTNA), שאוכף בדיקות אבטחה רציפות מבוססות הקשר.

B מקרה בוחן 2: הגבלת שער

פתרון למורה

הנחיות הערכה

תשובות התלמידים צריכות לכלול את הנקודות הבאות:

- ניתוח תרחיש: חברה מארחת מסדי נתונים פיננסיים פרטיים בענן. היא רוצה לחסום כל גישה ציבורית מהאינטרנט ללוחות הניהול ולאפשר התחברות רק מנקודות קצה מאומתות של החברה.
- אסטרטגיה ופתרון מומלצים: על מנהל המערכת להגדיר שער Dedicated IP ב-VPN הארגוני ולהוסיף את הכתובת הסטטית הזו לרשימה הלבנה בחומת האש של מסד הנתונים בענן.