الاسم: _____ التاريخ: _____ الدرجة: _____

دليل أكثر VPN أمانًا

تحليل تقني لتصميم VPN عالي الأمان، وخوادم الذاكرة المتطايرة العاملة بالذاكرة العشوائية فقط، وأمان الوصول بنهج انعدام الثقة، وحمايات تسرب DNS المشفر الخاص، وإعدادات WireGuard المدققة.

نظرة تعليمية على دليل أكثر VPN أمانًا

المتعلّم
حالة الطالب
مسار مدافع الشبكات

آمن
حالة الاتصال
حماية حزم البيانات

مُفعّل
الحماية من التسرّب
الحماية من تسرّب DNS وIPv6

مرحبًا! ترشدك حزمة الأنشطة هذه عبر المعايير التقنية لشبكات VPN عالية الأمان. ستستكشف عتاد الخوادم العاملة بذاكرة RAM فقط وأمان الوصول بانعدام الثقة ومحلّلات DNS الخاصة المشفّرة وإعدادات WireGuard المدققة.

نقاط التحقق في ورقة العمل

- ☐ **الجزء 1-4: أتقن إعدادات VPN وأمان الشبكات.**
- ☐ **الجزء 5-7: حل الكلمات المتقاطعة وألغاز البحث عن الكلمات.**
- ☐ **الجزء 8-9: حل دراسات الحالة وتحدي الشيفرة.**
- ☐ **الجزء 10: راجع صفحات الأسئلة الشائعة الأساسية والمتقدمة.**
- ☐ **الجزء 11: استكشف 10 حقائق مثيرة من الواقع.**
- ☐ **إضافي: تحدّي فكّر بسرعة**

افتح دليل VPN.com لأفضل شبكات VPN

URL: https://www.vpn.com/vpn/most-secure-vpn/

خارطة طريقك لتعلّم VPN الأكثر أمانًا

- حلّل البنية التقنية ومعايير التشفير في دليل Most Secure VPN.
- هيّئ إعدادات العميل لمنع تسريبات حركة IP وDNS وWebRTC.
- قارن بروتوكولات الأنفاق المملوكة لجهات بعينها بالتطبيقات القياسية.

تعليمات دليل أكثر VPN أمانًا

أجب عن أسئلة الاختيار من متعدد وأسئلة صحيح/خطأ، وأكمل الجمل الناقصة باستخدام بنك الكلمات، وطابق التعريفات، وحُلّ الكلمات المتقاطعة وبحث الكلمات. طبّق معرفتك على عتاد الخوادم العاملة بالذاكرة RAM فقط وأنظمة Zero Trust. واختم بالنشاط الإضافي «فكّر بسرعة».

البنى التحتية العاملة بالذاكرة العشوائية فقط وشبكات الثقة المعدومة (مقدمة)

يعتمد VPN الآمن حقًا على إطار الثقة المعدومة، وخوادم RAM فقط لمنع مصادرة الأقراص من كشف السجلات، ومحللات DNS مشفّرة خاصة، وبروتوكولات مدقَّقة مثل WireGuard. وتدافع هذه الضوابط مجتمعةً عن الأصول الرقمية عالية القيمة ضد تهديدات الاعتراض.

اقرأ كل نقطة تحقق بعناية، ثم اختر الإجابة الصحيحة أو اكتبها.

نقطة التحقق 1: تحدي الاختيار من متعدد

1. ما البنية الأساسية لضمان أعلى مستوى من الأمان في خوادم VPN الحديثة؟
   - A) بنية خوادم RAM فقط
   - B) تخزين قائم على الأقراص
   - C) توجيه DNS الديناميكي
   - D) تمكين إعادة توجيه المنافذ

2. ما البروتوكول الموصى به على نطاق واسع لأكثر إعدادات VPN أمانًا وحداثة؟
   - A) WireGuard
   - B) PPTP
   - C) L2TP/IPSec
   - D) SSTP

3. ما إطار الأمان الذي يتطلب التحقق من كل اتصال باستمرار دون استثناء؟
   - A) بنية الثقة المعدومة
   - B) جدران الحماية المحيطية
   - C) التوجيه الديناميكي
   - D) مفاتيح سرية مشتركة

4. ما الدور الرئيسي لحماية تسريب DNS في عميل VPN؟
   - A) توجيه جميع طلبات DNS عبر محللات خاصة مشفّرة
   - B) تعمية حزم IP
   - C) تخزين استعلامات DNS مؤقتًا محليًا
   - D) تعطيل خوادم الأسماء

5. كيف يزيد التوجيه متعدد القفزات الأمان الكلي لنفق VPN؟
   - A) يوجّه البيانات عبر خادمين منفصلين على التوالي
   - B) يزيد سرعة الضغط
   - C) يشفّر البيانات بشيفرات أمان منخفضة
   - D) يتجاوز جدران الحماية

نقطة التحقق 2: تحدي صحيح أم خطأ

6 سؤال 6

6. تخزّن الخوادم العاملة بالذاكرة العشوائية فقط ملفات السجلات في ذاكرة مؤقتة تُمحى عند إعادة التشغيل.

صحيح خطأ

7 سؤال 7

7. يستخدم WireGuard خوارزميات تشفير حديثة أقل عرضة لاختناقات السرعة.

صحيح خطأ

8 سؤال 8

8. يعمل مفتاح إيقاف VPN بحظر كل حركة مرور الشبكة إذا انقطع النفق.

صحيح خطأ

9 سؤال 9

9. عمليات التدقيق المستقلة من أطراف ثالثة لا صلة لها بالتحقق من الالتزامات الأمنية.

صحيح خطأ

10 سؤال 10

10. تفترض نماذج انعدام الثقة أن جميع اتصالات الشبكة الداخلية آمنة افتراضيًا.

صحيح خطأ

نقطة التحقق 3: إدراج المصطلحات الأساسية

اقرأ كل جملة أدناه وأكمل الفراغ بالمصطلح الصحيح من بنك الكلمات.

1. يفرض المسؤولون الأمان بنشر إطار صارم يقوم على مبدأ _____ الثقة.
2. يتطلب توجيه الحزم عبر نقاط دخول متعددة تهيئة آمنة متعددة _____ .
3. لمنع تسرب البيانات من الأقراص المسروقة، نستخدم تصميما يعتمد على _____ .
4. يخفف اختطاف مزود الإنترنت بتهيئة ميزات _____ الأصلية.
5. لحجب الحركة عند فشل الاتصال، فعل آلية _____ .
6. لتقليل سجلات قاعدة البيانات المخزنة، اختر مزودا _____ بالكامل.

بنك كلمات المفردات

الأسماء | التشفير | القفزات | انعدام | حماية DNS | خوادم الرام | مدققا | مفتاح الإيقاف

اكتب إجاباتك هنا:

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

نقطة التحقق 4: مطابقة مفاهيم VPN والشبكات

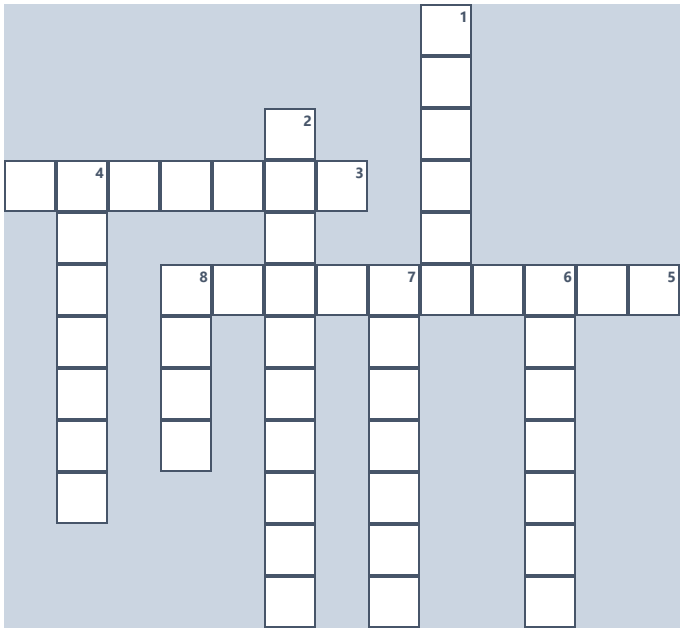
مطابقة التعريفات

طابق كل مصطلح مفردات على اليمين مع تعريفه الصحيح على اليسار بكتابة الحرف المقابل (A-H) في مربع الإدخال القابل للتعبئة.

1. انعدام الثقة	A	إعداد مفحوص بصورة مستقلة يؤكد عدم تخزين أي سجلات.
2. Multi-Hop	B	تعمية تشفيرية لحمولات البيانات لتأمين النقل.
3. خادم يعمل بالذاكرة العشوائية فقط	C	إطار أمني يتطلب المصادقة المستمرة لجميع المستخدمين.
4. حماية DNS	D	مجموعة من القواعد التقنية التي تحدد كيفية تعبئة البيانات وإرسالها.
5. Kill Switch	E	توجيه VPN المتسلسل الذي يربط عقدتي خادم معًا.
6. نظام خاضع للتدقيق	F	بنية خادم تستخدم ذاكرة متطايرة لتخزين حمولات البيانات.
7. التشفير	G	فرض استعلامات DNS الخاصة لحماية عمليات البحث في خوادم الأسماء.
8. البروتوكول	H	آلية آمنة عند الفشل تحجب حركة المرور إذا فشل VPN.

نقطة التحقق 5: لغز الكلمات المتقاطعة

حلّ الكلمات المتقاطعة بكتابة الحروف في المربعات البيضاء النشطة. تتوافق الأرقام مع الدلائل أدناه.



أفقي

3. فرض استعلامات DNS خاصة لحماية عمليات البحث عن عناوين النطاقات (7)

5. بنية خوادم تستخدم ذاكرة متطايرة لتخزين حمولات البيانات (10)

عمودي

1. إطار أمني يتطلب مصادقة مستمرة لجميع المستخدمين (6)

2. مجموعة قواعد تقنية تحدد كيفية تعبئة البيانات وإرسالها (10)

4. خلط تشفيري لحمولات البيانات لتأمين النقل (7)

6. آلية أمان احتياطية تحجب الحركة إذا تعطل VPN (7)

7. توجيه VPN متسلسل يربط عقدتي خادم معا (7)

8. إعداد فحصته جهات مستقلة وأكد عدم تخزين أي سجلات (4)

نقطة التحقق 5 – نشاط بديل: أدلة الكلمات المتقاطعة الميسَّرة

يمكن لمستخدمي قارئ الشاشة ولوحة المفاتيح كتابة إجابات الكلمات المتقاطعة مباشرة في حقول النص أدناه.

أفقي

3 أفقي: فرض استعلامات DNS خاصة لحماية عمليات البحث عن عناوين النطاقات (7 حروف):

5 أفقي: بنية خوادم تستخدم ذاكرة متطايرة لتخزين حمولات البيانات (10 حروف):

عمودي

1 عمودي: إطار أمني يتطلب مصادقة مستمرة لجميع المستخدمين (6 حروف):

2 عمودي: مجموعة قواعد تقنية تحدد كيفية تعبئة البيانات وإرسالها (10 حروف):

4 عمودي: خلط تشفيري لحمولات البيانات لتأمين النقل (7 حروف):

6 عمودي: آلية أمان احتياطية تحجب الحركة إذا تعطل VPN (7 حروف):

7 عمودي: توجيه VPN متسلسل يربط عقدتي خادم معا (7 حروف):

8 عمودي: إعداد فحصته جهات مستقلة وأكد عدم تخزين أي سجلات (4 حروف):

نقطة التحقق 6: البحث عن الكلمة المخفية

ابحث عن 8 مصطلحات مفردات رئيسية مخبأة في الشبكة أدناه. يمكن أن تكون الكلمات أفقية أو رأسية أو قطرية.

ت	ل	م	ز	د	ع	ك	ا	ط	ق	ي	ك	ف	ت	ن
م	م	ا	ح	س	س	ب	ل	ا	ا	ب	ت	ف	خ	س
ل	ش	د	خ	س	ي	ن	ت	ش	ل	ج	ك	ط	س	ج
و	ز	ع	ع	ع	ش	ك	ش	ق	ر	ق	ط	ط	ك	ل
ك	م	ن	ن	ن	خ	ر	ف	ت	م	ق	ف	ف	ا	ز
و	ل	ا	ب	و	و	ج	ي	م	ء	ه	ت	ز	ل	ء
ت	و	د	ش	ر	ا	ء	ر	ا	ج	ع	ج	ك	ا	ي
و	ق	ت	ن	ب	د	ا	ء	ل	ع	ج	س	ا	س	ت
ر	ج	ف	ج	ح	م	ر	ز	ا	ج	ل	ك	ط	م	ح
ب	ز	ل	ء	م	ا	م	ح	ي	ك	ه	ح	ا	ا	ا
ل	ك	ف	ع	ق	ل	د	ن	ق	ي	ك	ش	ل	ء	ن
ا	ل	ت	ع	خ	ر	ق	ب	ا	د	ل	ي	و	س	ا
ل	ء	خ	خ	س	ا	ق	د	ف	ز	ط	ك	ش	ط	ط
م	ف	ر	ق	ك	م	ر	ء	ا	ف	ه	د	ه	ب	خ
ل	خ	ب	ر	ط	ء	ر	ش	ف	ق	ع	ي	ت	ط	ء

قائمة كلمات المفردات

انعدام | القفزات | خوادمالرام | الاسماء | الايقاف | مدقق | التشفير | البروتوكول

نقطة التحقق 6 – نشاط بديل: مطابقة المفردات الميسَّرة

طابق كل مصطلح من المصطلحات الـ 8 في البحث عن الكلمات مع تعريفه الصحيح بكتابة الحرف (A-H) في الفراغ.

مصطلحات المفردات
A. انعدام
B. القفزات
C. خوادمالرام
D. الاسماء
E. الايقاف
F. مدقق
G. التشفير
H. البروتوكول

التعريفات وحقول المطابقة
1. آلية أمان احتياطية تحجب الحركة إذا تعطل VPN.
2. فرض استعلامات DNS خاصة لحماية عمليات البحث عن عناوين النطاقات.
3. توجيه VPN متسلسل يربط عقدتي خادم معا.
4. مجموعة قواعد تقنية تحدد كيفية تعبئة البيانات وإرسالها.
5. خلط تشفيري لحمولات البيانات لتأمين النقل.
6. بنية خوادم تستخدم ذاكرة متطايرة لتخزين حمولات البيانات.
7. إعداد فحصته جهات مستقلة وأكد عدم تخزين أي سجلات.
8. إطار أمني يتطلب مصادقة مستمرة لجميع المستخدمين.

نقطة التحقق 7: تحدي الكلمات المبعثرة

أعد ترتيب الحروف أدناه للكشف عن المفاهيم والمصطلحات الأساسية للشبكة الخاصة الافتراضية (VPN). اكتب إجاباتك في مربعات الإدخال المخصصة.

1. ع ا د ا م ن
2. ا د خ و م م ل ر ا ا
3. ي ا ق ف ا ا ل
4. ر ل ف ش ي ا ت
5. ز ت ف ق ا ا ل
6. ا ا م ا س ء ل
7. ق م ق د
8. و ر ت ل ا و ل و ك ب

نشاط إضافي: فكّر بسرعة

اكتب 3 إجابات لكل فئة. يفوز أول من يكمل القائمة.

1	أقفال أو مفاتيح تستخدمها كل يوم		
2	أشياء يمكن أن يخفيها VPN		
3	أشياء تجعل VPN آمنًا		
4	خرافات عن VPN		
5	أسباب لاستخدام VPN أثناء السفر		
6	أماكن آمنة في العالم الواقعي		
7	كلمات تعني "محمي"		
8	وعود يقدمها مزوّد VPN جيد		
9	كلمات متعلقة بالخصوصية		
10	أنواع التدقيق أو الفحص		
11	كلمات من ورقة العمل هذه تريد تذكّرها		
12	أشياء يريد المخترق سرقتها		
13	طرق لاكتشاف شبكة Wi-Fi مزيفة		
14	أماكن تستخدم فيها VPN		
15	أشياء يستطيع مزوّد الإنترنت رؤيتها		

نقطة التحقق 8: دراسات حالة في VPN والشبكات

طبّق المفاهيم التي تعلمتها لحل السيناريوهات الواقعية أدناه.

دراسة الحالة 1: تحصين البنية التحتية للمؤسسات

👷

السيناريو: يعيد بنك مؤسسي تصميم طوبولوجيا الوصول عن بُعد. يحتاج إلى بنية الثقة المعدومة (Zero Trust) تربط جميع أجهزة العملاء بخوادم آمنة.

سؤال للنقاش: ما الفائدة الرئيسية للتجزئة الدقيقة للشبكة في نموذج VPN القائم على الثقة المعدومة؟

دراسة الحالة 2: حمايات الخوادم العاملة بالذاكرة RAM فقط

👷

السيناريو: يطوّر مزوّد VPN يركز على الأمان خوادمه لمنع المصادرة المادية للخوادم من كشف سجلات المستخدمين.

سؤال للنقاش: اشرح كيف تمنع تهيئات الأجهزة التي تعمل بذاكرة RAM فقط استخراج البيانات الجنائية أثناء المصادرة المادية للخوادم.

نقطة التحقق 9: فك الشيفرة

يؤمّن مهندس الشبكات قنوات التوجيه وأنفاق العملاء. استخدم مفتاح الحرف إلى الرقم أدناه لفك تشفير الرسالة بكتابة الحروف المطابقة في الفراغات.

مفتاح التشفير من الحرف إلى الرقم

ا=1 ب=2 ت=3 ث=4 ج=5 ح=6 خ=7 د=8 ذ=9 ر=10 ز=11

س=12 ش=13 ص=14 ض=15 ط=16 ظ=17 ع=18 غ=19 ف=20 ق=21 ك=22

ل=23 م=24 ن=25 هـ=26 و=27 ي=28 ة=29 ى=30 ء=31 ؤ=32 ئ=33

25	24	32	3		29	25	24	1	23	1		3	1	22	2	13	23	1

29	24	28	21	23	1		29	28	24	21	10	23	1		23	27	14	1	23	1

الرسالة بعد فك التشفير:

نصيحة: يمثل كل رقم حرفًا عربيًا واحدًا من المفتاح أعلاه.

نقطة التحقق 10: الأسئلة الشائعة الأساسية حول VPN (الجزء A)

راجع الأسئلة والأجوبة الأكثر شيوعًا حول الشبكات الخاصة الافتراضية (VPN) والأنفاق.

Q1: ما الذي يجعل VPN "الأكثر أمانًا"؟

مزيج من الثقة المعدومة وخوادم RAM فقط والبروتوكولات المدقَّقة.

Q2: ما الخوادم العاملة بالذاكرة العشوائية فقط؟

خوادم تعمل في الذاكرة المتطايرة، مصممة بحيث لا تخزّن أي سجلات على القرص.

Q3: ما VPN الثقة المعدومة (Zero Trust)؟

إطار عمل يتحقق باستمرار من كل طلب وصول واتصال.

Q4: لماذا يُعد WireGuard آمنًا؟

لديه قاعدة شيفرة صغيرة يسهل تدقيقها ويستخدم شيفرات حديثة.

Q5: كيف تمنع شبكات VPN الآمنة تسريبات DNS؟

بتوجيه جميع الاستعلامات عبر محللات DNS خاصة ومشفّرة.

نقطة التحقق 10: الأسئلة الشائعة الأساسية حول VPN (الجزء B)

راجع الأسئلة والأجوبة الأكثر شيوعًا حول الشبكات الخاصة الافتراضية (VPN) والأنفاق.

Q6: هل يتطلب VPN الآمن عمليات تدقيق؟

نعم، تتحقق عمليات التدقيق المستقلة من ادعاءات عدم الاحتفاظ بالسجلات ومن أمان الشيفرة.

Q7: ما دور مفتاح الإيقاف؟

يوقف حركة الشبكة فورًا إذا انقطع اتصال VPN.

Q8: ما التشفير المستخدم في شبكات VPN الآمنة؟

يُعدّ AES-256 وChaCha20 المعيارين الصناعيين للتشفير.

Q9: هل التوجيه متعدد القفزات (Multi-Hop) آمن؟

نعم، يربط خادمين أو أكثر على التسلسل لمنع تحليل حركة البيانات.

Q10: كيف يفيد الاختصاص القضائي الخارجي؟

قد يحدّ من القوانين السارية، لكنه لا يوفر حصانة مطلقة.

نقطة التحقق 10: الأسئلة الشائعة المتقدمة حول VPN (الجزء C)

استكشف الجوانب التقنية المتقدمة لبروتوكولات أنفاق VPN وتكامل عملاء الجوال ونشر المؤسسات.

Q1: كيف تمنع الخوادم العاملة بالذاكرة العشوائية فقط مخاطر مصادرة البيانات؟

لأنها تعمل في الذاكرة RAM، فإن فصل الطاقة يمسح البيانات المحفوظة في الذاكرة.

Q2: كيف يحل Zero Trust محل أمان المحيط القياسي؟

يعامل كل عميل على أنه معادٍ، ويتطلب مصادقة مستمرة.

Q3: ما الذي يجعل شيفرة WireGuard المصدرية أسهل في التدقيق؟

شيفرته على Linux أقل من 4,000 سطر، أصغر بكثير من حزم VPN المعتادة. [4]

Q4: كيف يحمي DNSSEC استعلامات DNS؟

يوقّع سجلات DNS بحيث تتمكن المحللات من اكتشاف الإجابات المزوّرة أو المتلاعب بها.

Q5: كيف يعقّد Multi-Hop ربط الحركة ببعضها؟

بفصل عناوين IP الواردة والصادرة عبر مزودي استضافة مختلفين.

نقطة التحقق 10: الأسئلة الشائعة المتقدمة حول VPN (الجزء D)

استكشف الجوانب التقنية المتقدمة لبروتوكولات أنفاق VPN وتكامل عملاء الجوال ونشر المؤسسات.

Q6: لماذا تُعد ولايات تحالف العيون الخمس (Five Eyes) القضائية محفوفة بالمخاطر لشبكات VPN؟

تتبادل الدول الأعضاء المعلومات الاستخباراتية وقد تستخدم أوامر قانونية لطلب بيانات المستخدمين.

Q7: كيف يُنفَّذ مفتاح الإيقاف على مستوى النواة؟

يستخدم قواعد جدار حماية النظام (مثل iptables أو WFP) لحجب الحركة الصادرة.

Q8: ما السرية الأمامية في مصافحات VPN؟

يولّد مفاتيح جلسات فريدة بحيث لا يمكن فك تشفير الجلسات السابقة.

Q9: كيف تخفف شبكات VPN الآمنة من تسريبات WebRTC؟

بحظر طلبات WebRTC أو توجيهها عبر النفق.

Q10: كيف تضمن عمليات التدقيق المستقلة الامتثال للخصوصية؟

يجري المدققون اختبارات الاختراق ويفحصون إعدادات الخوادم.

الجزء 11: 10 حقائق ورؤى واقعية عن VPN

راجع حقائق واقعية عن سرعات تشفير VPN وتدقيق البروتوكولات والاتصال عبر الجوال والعمل عن بُعد في المؤسسات.

1. نظرة على VPN

تحمّل الخوادم العاملة بالذاكرة العشوائية فقط نظام التشغيل في الذاكرة عند الإقلاع، فلا يبقى شيء على القرص بعد إعادة التشغيل.

2. نظرة على VPN

يستخدم WireGuard إطار Noise مع Curve25519 وChaCha20 وPoly1305 وBLAKE2s وHKDF. [3]

3. نظرة على VPN

يمنح انعدام الثقة الوصول لكل مورد على حدة ولا يمنح أي ثقة ضمنية بناءً على موقع الشبكة (NIST SP 800-207). [1]

4. نظرة على VPN

يضم تحالف Five Eyes الاستخباراتي الولايات المتحدة والمملكة المتحدة وكندا وأستراليا ونيوزيلندا.

5. نظرة على VPN

تحدث تسريبات WebRTC عندما تكشف المتصفحات عنوان IP العام الحقيقي للعميل عبر استعلامات STUN.

6. نظرة على VPN

تضمن السرية المستمرة الكاملة (PFS) ألا يؤدي اختراق مفتاح طويل الأمد إلى كشف مفاتيح الجلسات السابقة. [3]

7. رؤية حول VPN

نشرت Cure53، وهي شركة أمنية مقرها برلين، تدقيقات لعدة مزودي VPN.

8. رؤية حول VPN

يحدث تسرّب DNS عندما تتجاوز استعلامات DNS نفق VPN وتذهب إلى خوادم الأسماء التابعة لمزوّد خدمة الإنترنت المحلي.

9. رؤية حول VPN

تحتاج شرائح الذاكرة العشوائية المتطايرة إلى طاقة كهربائية مستمرة للاحتفاظ بالبيانات، وتفقد محتوياتها عند انقطاع الطاقة.

10. نظرة على VPN

تفرض أنظمة انعدام الثقة في المؤسسات فحوص وضع الجهاز قبل السماح بالاتصال بالموارد الآمنة. [1]

المراجع والمصادر التقنية

أُعد دليل الدراسة والألغاز التفاعلية استنادًا إلى المعايير والمواصفات التقنية العالمية والأطر التنظيمية.

المراجع الأكاديمية والصناعية

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

[2] WireGuard. (n.d.). WireGuard: fast, modern, secure VPN tunnel.
https://www.wireguard.com/

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

[4] 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/

[5] NIST. (2020). SP 800-77 Rev. 1: Guide to IPsec VPNs.
https://csrc.nist.gov/pubs/sp/800/77/r1/final

[6] OpenVPN. (n.d.). OpenVPN 2.6 Manual.
https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/

مفتاح الإجابة: نقطة التحقق 1 - اختيار من متعدد

1 خادم يعمل بالذاكرة العشوائية فقط — الذاكرة العشوائية فقط — الإجابة الصحيحة: A

ملاحظة للمعلم

لا تخزّن الخوادم العاملة بالذاكرة العشوائية فقط أي سجلات على القرص، وتُمحى البيانات عند إعادة التشغيل. المصدر: Most Secure VPN.

2 السؤال 2 — الإجابة الصحيحة: A

ملاحظة للمعلم

يجمع WireGuard بين قاعدة شيفرة صغيرة قابلة للتدقيق وشيفرات حديثة.

3 نموذج انعدام الثقة — انعدام الثقة — الإجابة الصحيحة: A

ملاحظة للمعلم

تتحقق نماذج انعدام الثقة من امتثال الجهاز باستمرار قبل منح الوصول. الاستشهاد: Most Secure VPN.

4 حماية DNS — حماية DNS — الإجابة الصحيحة: A

ملاحظة للمعلم

تُوجّه الحماية من تسرّب DNS استعلامات البحث عبر مُحلّلات خاصة. المصدر: Most Secure VPN.

5 أنفاق Multi-Hop — MULTI-HOP — الإجابة الصحيحة: A

ملاحظة للمعلم

يسلسل توجيه Multi-Hop عقدتي خادم منفصلتين على التوالي. المصدر: Most Secure VPN.

مفتاح الإجابة: نقطة التحقق 2 - صحيح أو خطأ

6 خادم يعمل بالذاكرة العشوائية فقط — الذاكرة العشوائية فقط

الإجابة الصحيحة: صحيح

ملاحظة للمعلم

لا يكتب عتاد الخادم العامل بالذاكرة العشوائية فقط أي بيانات على القرص، وتُمحى البيانات عند إعادة التشغيل. المصدر: Most Secure VPN.

7 سرعة WireGuard — WIREGUARD

الإجابة الصحيحة: صحيح

ملاحظة للمعلم

يستخدم WireGuard تشفيرًا حديثًا يتجنب اختناقات المعالجة. الاستشهاد: Most Secure VPN.

8 Kill Switch — مفتاح الأمان عند الفشل

الإجابة الصحيحة: صحيح

ملاحظة للمعلم

يحظر مفتاح الإيقاف كل حركة المرور إذا انقطع اتصال VPN. المصدر: Most Secure VPN.

9 عمليات تدقيق الأطراف الثالثة — التدقيقات ضرورية

الإجابة الصحيحة: خطأ

ملاحظة للمعلم

تُعد عمليات تدقيق الأطراف الثالثة ضرورية للتحقق من ادعاءات الخصوصية لدى الشركات. المرجع: Most Secure VPN.

10 السؤال 10

الإجابة الصحيحة: خطأ

ملاحظة للمعلم

لا تمنح الثقة المعدومة (Zero Trust) أي ثقة ضمنية بناءً على موقع الشبكة.

مفاتيح المفردات ومعيار التقييم

معيار التصحيح للمعلم: امنح 1 نقطة لكل مطابقة صحيحة (المجموع 8 نقطة) ولكل مصطلح سياق (المجموع 6 نقطة).

نقطة التحقق 4: مفتاح الإجابة – مطابقة المفاهيم

C 1. انعدام الثقة	E 2. Multi-Hop	F 3. خادم يعمل بالذاكرة العشوائية فقط	G 4. حماية DNS
H 5. Kill Switch	A 6. نظام خاضع للتدقيق	B 7. التشفير	D 8. البروتوكول

نقطة التحقق 3: مفتاح الإجابة – المصطلحات الأساسية

1 انعدام	2 القفزات	3 خوادم الرام	4 حماية DNS
5 مفتاح الإيقاف	6 مدققا		

نقطة التحقق 6 – نشاط بديل: مفتاح الإجابة – مطابقة المفردات

1 E – الايقاف	2 D – الاسماء	3 B – القفزات	4 H – البروتوكول
5 G – التشفير	6 C – خوادمالرام	7 F – مدقق	8 A – انعدام

ملاحظات النقاش للمعلمين

المصطلحات الأساسية:
تحقّق من قدرة الطلاب على شرح انعدام الثقة وMulti-Hop وخادم يعمل بالذاكرة العشوائية فقط بكلماتهم الخاصة وإعطاء مثال على كل منها.

دراسات الحالة:
اطلب من الطلاب أن يدعموا توصياتهم بحقائق من ورقة العمل لا بآرائهم.

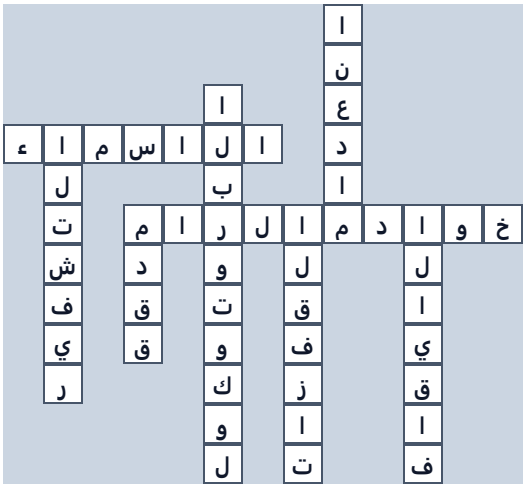
تقييم المصادر:
اطلب من الطلاب التحقق من ادعاء واحد على الأقل من مراجع ورقة العمل، وناقش لماذا قد تتغير الأرقام والأسعار والقواعد مع الوقت.

مفاتيح الألغاز وملاحظات المعلم

حل البحث عن الكلمات

ت	ل	م	ز	د	ع	ك	ا	ط	ق	ي	ك	ف	ت	ن
م	م	ا	ح	ص	س	ب	ل	ا	ا	ب	ت	ف	خ	ص
ل	ش	د	خ	ص	ي	ن	ت	ش	ل	ج	ك	ط	س	ج
و	ز	ع	ع	ش	ك	ق	ش	ق	ر	ق	ط	ط	ك	ل
ك	م	ن	ن	خ	ر	ف	ت	م	ق	ف	ف	ا	ل	ز
و	ل	ا	ب	و	و	ي	م	ء	ه	ت	ز	ل	ا	ء
ت	و	د	ش	ر	ا	ء	ر	ا	ج	ج	ع	ج	ا	ي
و	ق	ت	ن	ب	د	ا	ل	ع	ج	ع	س	ا	س	ت
ر	ج	ف	ج	ح	م	ر	ز	ا	ج	ل	ك	ط	م	ح
ب	ز	ل	م	ء	ا	م	ي	ك	ه	ح	ا	ا	ا	ا
ل	ك	ف	ع	ق	ل	د	ن	ق	ي	ك	ش	ل	ء	ن
ا	ل	ت	خ	ع	ت	ق	ا	ب	د	ل	ي	و	س	ا
ل	ء	خ	خ	ص	ا	ق	ف	د	ز	ط	ك	ش	ط	ط
م	ف	ر	ق	ك	م	ر	ء	ا	ف	ه	د	ه	ب	خ
ل	خ	ب	ر	ط	ء	ش	ر	ف	ق	ع	ي	ت	ط	ء

حل الكلمات المتقاطعة



دليل المعلم لحلول الكلمات المتقاطعة

أفقي

3 أفقي: الاسماء فرض استعلامات DNS خاصة لحماية عمليات البحث عن عناوين النطاقات (7 حروف)

5 أفقي: خوادمالرام بنية خوادم تستخدم ذاكرة متطايرة لتخزين حمولات البيانات (10 حروف)

عمودي

1 عمودي: انعدام إطار أمني يتطلب مصادقة مستمرة لجميع المستخدمين (6 حروف)

2 عمودي: البروتوكول مجموعة قواعد تقنية تحدد كيفية تعبئة البيانات وإرسالها (10 حروف)

4 عمودي: التشفير خلط تشفيري لحمولات البيانات لتأمين النقل (7 حروف)

6 عمودي: الايقاف آلية أمان احتياطية تحجب الحركة إذا تعطل VPN (7 حروف)

7 عمودي: القفزات توجيه VPN متسلسل يربط عقدتي خادم معا (7 حروف)

8 عمودي: مدقق إعداد فحصته جهات مستقلة وأكد عدم تخزين أي سجلات (4 حروف)

مفتاح حل الكلمات المبعثرة والشيفرة

مفتاح تصحيح لنشاط فك خلط مفردات المصطلحات وتحدي الشيفرة السرية.

مفتاح ترتيب الكلمات المبعثرة

1. عادامن — انعدام
2. ادخوملرالا — خوادمالرام
3. ياقفال — الايقاف
4. رلفشيات — التشفير
5. زتفقال — القفزات
6. االماسءل — الاسماء
7. قمقد — مدقق
8. ورتلاولوكب — البروتوكول

مفتاح تحدي الشيفرة السرية

"الشبكات الآمنة تؤمن الأصول الرقمية القيمة"

مفتاح إجابات دراسات الحالة

A دراسة الحالة 1: تحصين البنية التحتية للمؤسسات

حل المعلم

دليل التصحيح

ينبغي أن تغطي إجابات الطلاب النقاط التالية:

- تحليل السيناريو: يعيد بنك مؤسسي تصميم طوبولوجيا الوصول عن بُعد. ويتطلب بنية انعدام الثقة تربط جميع أجهزة العملاء بالخوادم الآمنة.
- الاستراتيجية والحل الموصى بهما: إرشادات التصحيح: اشرح أن التجزئة الدقيقة (micro-segmentation) تحصر الوصول في موارد محددة، فتمنع الحركة الجانبية للتهديدات إذا تعرض جهاز للاختراق.

B دراسة الحالة 2: حمايات الخوادم العاملة بالذاكرة RAM فقط

حل المعلم

دليل التصحيح

ينبغي أن تغطي إجابات الطلاب النقاط التالية:

- تحليل السيناريو: يطوّر مزود VPN يركز على الأمان خوادمه لمنع مصادرة الخوادم ماديًا من كشف سجلات المستخدمين التاريخية.
- الاستراتيجية والحل الموصى بهما: إرشادات التصحيح: وضّح أن خوادم RAM-Only لا تحتوي على تخزين قرصي مادي. وأن انقطاع الطاقة يمسح تلقائيًا جميع البيانات المؤقتة في الذاكرة المتطايرة.