الاسم: _____ التاريخ: _____ الدرجة: _____

دليل VPN.com لـ VPN
ورقة العمل

تمارين عملية في بروتوكولات الشبكات والأنفاق وضوابط الأمان.

نظرة تعليمية عامة على VPN

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 المبادئ الأساسية للشبكات الخاصة الافتراضية (VPN). ستستكشف كيف تؤمّن الأنفاق المشفّرة بياناتك، وكيف تعمل بروتوكولات الشبكة، وكيف تحدد تسرّبات الخصوصية وتخفف منها.

نقاط التحقق في ورقة العمل

- ☐ **الجزء 1-4: أتقن مفاهيم VPN وبروتوكولاته.**
- ☐ **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 لشبكات VPN

URL: https://www.vpn.com/vpn/

خارطة طريقك لتعلّم VPN

- اشرح مفهوم نفق البيانات والتغليف.
- تعرّف على إعدادات البروتوكولات القياسية ومتطلبات عرض النطاق الترددي.
- حلّل أدوار جدران الحماية والحجب الجغرافي في توجيه الإنترنت.
- افهم كيف تتتبع مزودات خدمة الإنترنت التصفح غير المشفر وكيف يمنع VPN ذلك.
- ميّز الحدود التشغيلية لموقع الخادم والولاية القضائية.

تعليمات دليل VPN

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 سيناريوهات حقيقية في قسم دراسات الحالة. واختم بالنشاط الإضافي «فكّر بسرعة».

ما هي VPN؟ (مقدمة)

الشبكة الخاصة الافتراضية أكثر من مجرد مفتاح للخصوصية. إنها نفق مشفّر يوجّه حركة الإنترنت عبر خادم بعيد. وهذا يخفي عنوان IP الخاص بك، ويمنع مزوّد الإنترنت من تجميع سجلات لأنشطتك على الإنترنت، ويؤمّن بياناتك على الشبكات العامة. وفهم المصطلحات أمر أساسي للحفاظ على السلامة الرقمية.

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

نقطة التحقق 1: تحدي الاختيار من متعدد

1. 1. ما هو بروتوكول VPN؟
   - A. جهاز عتادي يُستخدم لتوصيل الكابلات.
   - B. مجموعة قواعد تحدد كيفية تشفير البيانات وإرسالها.
   - C. إضافة متصفح تحظر الإعلانات.
   - D. شركة مزودة لخدمة الإنترنت.

2. 2. إذا بدا اتصال VPN بطيئًا، فما السبب الأرجح؟
   - A. خادم VPN بعيد جدًا أو محمَّل فوق طاقته.
   - B. دقة شاشة العرض لديك مضبوطة على قيمة مرتفعة جدًا.
   - C. لقد عطّلت ملفات تعريف الارتباط في متصفح الويب.
   - D. تخطيط لوحة المفاتيح لديك مهيأ بشكل غير صحيح.

3. 3. لماذا يُوصى بشدة باستخدام VPN عند الاتصال بشبكة Wi-Fi عامة؟
   - A. يجعل اتصال Wi-Fi مجانيًا.
   - B. يزيد نطاق تغطية الموجّه.
   - C. يشفّر حركة البيانات لمنع المخترقين على الشبكة نفسها.
   - D. يحذف رسائل البريد الإلكتروني غير المرغوب فيها تلقائيًا.

4. 4. أي مما يلي يصف الحجب الجغرافي؟
   - A. أداة تقيس المسافة الفعلية إلى الخادم.
   - B. قيد يحجب الوصول إلى الموقع بحسب الموقع الجغرافي.
   - C. بروتوكول لضغط الملفات المحلية.
   - D. آلية تخزين للنسخ الاحتياطي.

5. 5. ماذا يستطيع مزود خدمة الإنترنت (ISP) أن يراه عند استخدامك VPN؟
   - A. كلمات البحث ومحتوى صفحات الويب التي تعرضها.
   - B. أنك متصل بشبكة VPN، دون تفاصيل حركة المرور.
   - C. لا معلومات، ولا حتى أنك متصل بالإنترنت.
   - D. ملفاتك وصورك على القرص الصلب المحلي.

نقطة التحقق 2: تحدي صحيح أم خطأ

6 إخفاء الموقع

6. يخفي VPN عنوان IP العام لجهازك، فيمنع مواقع الأطراف الثالثة من تحديد موقعك الفعلي بسهولة.

صحيح ○ خطأ ○

7 أثر VPN في السرعة

7. يجعل تفعيل اتصال VPN سرعة الإنترنت الأساسية لديك ضعف سرعة اتصالك دون VPN.

صحيح ○ خطأ ○

8 التنصت على Wi-Fi العام

8. إذا استخدمت شبكة Wi-Fi عامة غير مؤمنة دون VPN، فقد يتمكن مستخدمون آخرون على الشبكة نفسها من التقاط حركة بياناتك غير المشفرة.

صحيح ○ خطأ ○

9 جدران الحماية والاتصالات المحجوبة

9. يمكن لمسؤولي الشبكات ضبط جدران الحماية لاكتشاف أنفاق اتصال VPN الصادرة وحجبها.

صحيح ○ خطأ ○

10 سياسات صارمة لعدم الاحتفاظ بالسجلات

10. تعني سياسة "عدم الاحتفاظ بالسجلات" الصارمة أن مزوّد VPN ملزم قانونيًا بتخزين استعلامات البحث والروابط التي زرتها لمدة 30 يومًا على الأقل.

صحيح ○ خطأ ○

نقطة التحقق 3: إدراج المصطلحات الأساسية

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

1. لتأمين حركتك، يلف VPN حزم بياناتك داخل بروتوكول آخر في عملية تعرف باسم _____ .
2. إذا واجهت سرعات تنزيل بطيئة أثناء البث، فقد يكون ذلك بسبب محدودية _____ المتاح في الشبكة.
3. تستخدم خدمة بث متاحة في بلد معين فقط الحجب _____ لتقييد المستخدمين عالميا.
4. تسمى قواعد الاتصال التي تحدد معاملات التشفير والاتصال _____ VPN.
5. يستخدم حاسوبك _____ محليا لمراقبة حركة الشبكة وحجب الاتصالات غير الآمنة.
6. عند الاتصال بـ VPN، توجه بياناتك عبر _____ بعيد لإخفاء عنوان IP العام.

بنك كلمات المفردات

التغليف الجغرافي الخصوصية بروتوكول مزود الخدمة جدار حماية خادم عرض النطاق

اكتب إجاباتك هنا:

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

نقطة التحقق 4: مطابقة مفاهيم الشبكات

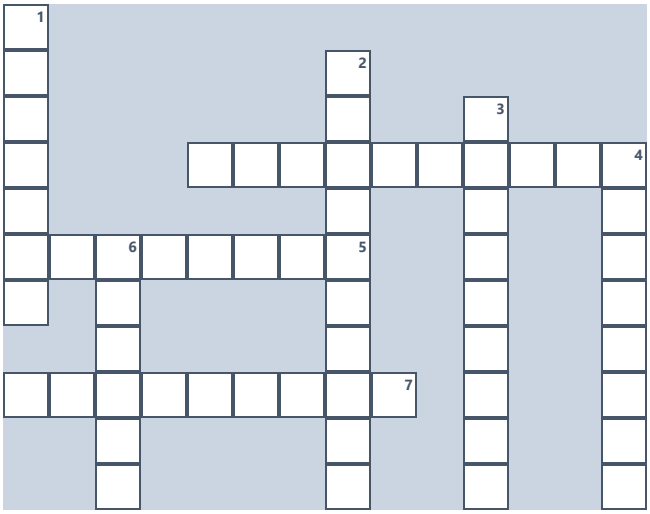
مطابقة التعريفات

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

1. النفقة	A	مجموعة قواعد تحدد كيفية إرسال البيانات عبر الشبكة.
2. البروتوكول	B	أقصى معدل لنقل البيانات عبر اتصال ما.
3. النطاق الترددي	C	قيد يمنع الوصول إلى الويب بناءً على الموقع الجغرافي.
4. الخادم	D	نظام أمان يراقب حركة المرور غير المصرّح بها ويحظرها.
5. الحظر الجغرافي	E	حاسوب بعيد يوجّه حركتك ويخفي عنوان IP الخاص بك.
6. جدار الحماية	F	حالة التحرر من التتبع أو المراقبة العامة.
7. الخصوصية	G	مزوّد خدمة الإنترنت الذي ينقل حركة بياناتك ويمكنه رؤية النشاط غير المشفر.
8. مزوّد الإنترنت	H	تغليف حزم البيانات داخل حزمة أخرى للنقل الآمن.

نقطة التحقق 5: لغز الكلمات المتقاطعة

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



أفقي

4. مجموعة قواعد تحدد كيفية إرسال البيانات عبر الشبكة (10)

5. قيد يمنع الوصول إلى الويب بحسب الموقع المادي (8)

7. نظام أمان يراقب الحركة غير المصرح بها ويحجبها (9)

عمودي

1. لف حزم البيانات داخل حزمة أخرى للنقل الآمن (7)

2. مزود خدمة الإنترنت الذي يسجل حركتك ما لم تكن مشفرة (10)

3. أقصى معدل لنقل البيانات عبر الاتصال (9)

4. حالة التحرر من التتبع أو المراقبة العامة (8)

6. حاسوب بعيد يوجه حركتك ويخفي عنوان IP الخاص بك (6)

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

4 أفقي: مجموعة قواعد تحدد كيفية إرسال البيانات عبر الشبكة (10 حروف):

5 أفقي: قيد يمنع الوصول إلى الويب بحسب الموقع المادي (8 حروف):

7 أفقي: نظام أمان يراقب الحركة غير المصرح بها ويحجبها (9 حروف):

عمودي

1 عمودي: لف حزم البيانات داخل حزمة أخرى للنقل الآمن (7 حروف):

2 عمودي: مزود خدمة الإنترنت الذي يسجل حركتك ما لم تكن مشفرة (10 حروف):

3 عمودي: أقصى معدل لنقل البيانات عبر الاتصال (9 حروف):

4 عمودي: حالة التحرر من التتبع أو المراقبة العامة (8 حروف):

6 عمودي: حاسوب بعيد يوجه حركتك ويخفي عنوان IP الخاص بك (6 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.

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

قائمة كلمات المفردات

التغليف البروتوكول عرضالنطاق الخادم مزودالخدمة الجغرافي جدارحماية الخصوصية

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. التغليف
B. البروتوكول
C. عرضالنطاق
D. الخادم
E. الجغرافي
F. جدارحماية
G. الخصوصية
H. مزودالخدمة

التعريفات وحقول المطابقة
1. حالة التحرر من التتبع أو المراقبة العامة.
2. قيد يمنع الوصول إلى الويب بحسب الموقع المادي.
3. مجموعة قواعد تحدد كيفية إرسال البيانات عبر الشبكة.
4. نظام أمان يراقب الحركة غير المصرح بها ويحجبها.
5. أقصى معدل لنقل البيانات عبر الاتصال.
6. حاسوب بعيد يوجه حركتك ويخفي عنوان IP الخاص بك.
7. مزود خدمة الإنترنت الذي يسجل حركتك ما لم تكن مشفرة.
8. لف حزم البيانات داخل حزمة أخرى للنقل الآمن.

نقطة التحقق 7: تحدي الكلمات المبعثرة

أعد ترتيب الحروف أدناه للكشف عن مفاهيم ومصطلحات VPN الأساسية. اكتب إجاباتك في مربعات الإدخال القابلة للتعبئة.

1. غ ي ا ل ف ت ل
2. ق ع ا ا ر ن ط ل ض
3. غ ل ا ر ا ي ف ج
4. ص ي ة ص و ا ل خ
5. ك ت ل ل ر و و ا و ب
6. د ا ا خ م ل
7. م ج ي ة ا ر د ح ا
8. م د ل ة م ا ز خ د و

نشاط إضافي: فكّر بسرعة

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

1	أشياء ترتبط في ذهنك بكلمة "نفق"		
2	أشياء تعلّمها عائلتك عن VPN		
3	أشياء في الموقع الإلكتروني يمكن أن تتتبعك		
4	خرافات عن VPN		
5	كلمات من ورقة العمل هذه تريد تذكّرها		
6	أجهزة يمكنها استخدام VPN		
7	أشياء لا يحميك منها VPN		
8	دول تودّ "زيارتها" عبر الإنترنت		
9	وعود يقدمها مزوّد VPN جيد		
10	طرق لاكتشاف شبكة Wi-Fi مزيفة		
11	أسئلة لديك عن VPN		
12	خدمات VPN التي تعرفها		
13	كلمات متعلقة بالخصوصية		
14	أشياء يمكن أن يخفيها VPN		
15	أسباب لاستخدام VPN في مقهى		

نقطة التحقق 8: دراسات حالة في VPN

طبّق المفاهيم التي تعلمتها لحل السيناريوهات الواقعية أدناه.

سارة (طالبة المقهى)

👩‍💻 "مرحبًا! أجلس في Coffee & Bytes. توجد شبكة عامة غير مؤمّنة اسمها 'Free_Wi-Fi_No_Password'. أريد تسجيل الدخول إلى بريد مدرستي الإلكتروني ورفع واجبي، لكنني قلق من المخترقين. ما مخاطر استخدام هذه الشبكة دون VPN، وكيف يؤمّن VPN بياناتي؟"

ALEX (طالب مسافر)

👨‍💻 "يا للأسف! أسافر إلى الخارج لإنجاز مشروع وأحاول مشاهدة فيلم وثائقي عن الأحياء مستضاف على خادم في بلدي. لكن الموقع يقول: 'هذا الفيديو غير متاح في موقعك الحالي.' لماذا أُحظر، وكيف يمكن لـ VPN مساعدتي في مشاهدته؟"

نقطة التحقق 9: فك الشيفرة

يشفّر VPN حركة مرورك لتأمينها. استخدم مفتاح الحرف إلى الرقم أدناه لفك تشفير رسالة الأمن السيبراني 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	1		21	20	25	2		22	3	28	14	27	14	7		24	6	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 لدى العملاء المحتملين حول استخدام الشبكات الخاصة الافتراضية.

Q1: ما VPN وكيف يعمل؟

تشفّر الشبكة الخاصة الافتراضية (VPN) اتصالك بالإنترنت وتوجّه حركة مرورك عبر خادم بعيد آمن. وهذا يخفي عنوان IP العام الخاص بك ويحدّ مما يستطيع مراقبو الشبكة المحلية ومزوّد الإنترنت رؤيته عن الحركة الموجَّهة عبر نفق VPN.

Q2: لماذا ينبغي لي استخدام VPN؟

يحمي VPN خصوصيتك الرقمية، ويؤمّن اتصالك على شبكات Wi-Fi العامة (مثل المقاهي أو المطارات)، وقد يقلّل الخنق القائم على النشاط عندما لا يستطيع مزوّد الإنترنت تحديد نوع الحركة المشفّرة، ويتجاوز القيود الجغرافية للوصول إلى المحتوى العالمي، ويساعد في تأمين موارد العمل عن بُعد.

Q3: هل يجعلني VPN مجهول الهوية تمامًا على الإنترنت؟

لا. فرغم أن VPN يخفي عنوان IP ويشفّر حركة المرور، لا يزال بالإمكان تتبعك عبر ملفات تعريف ارتباط المتصفح، أو الحسابات النشطة (مثل Google أو Facebook)، أو بصمة المتصفح، أو إذا كان مزود VPN يسجل بياناتك.

Q4: هل سيبطئ VPN سرعة الإنترنت لدي؟

نعم، قليلًا. تضيف عملية التشفير والمسافة المادية إلى خادم VPN زمن استجابة وحملًا إضافيًا. ويختلف الأثر بحسب المزوّد والبروتوكول ومسافة الخادم والجهاز وظروف الشبكة.

Q5: هل استخدام VPN قانوني؟

استخدام VPN قانوني في دول كثيرة، لكن بعض الاختصاصات القضائية تقيّد خدمات VPN أو تنظمها أو تحظرها. ينبغي للمستخدمين التحقق من القوانين المحلية السارية قبل الاستخدام. لمزيد من التفاصيل، راجع أدلة الوضع القانوني على VPN.com.

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

راجع الأسئلة والأجوبة الأكثر شيوعًا لدى العملاء المحتملين حول استخدام الشبكات الخاصة الافتراضية.

Q6: هل يمكنني استخدام VPN مجاني؟

قد تعتمد خدمات VPN المجانية على الإعلانات أو الميزات المحدودة أو تحليلات الاستخدام أو حدود البيانات أو نماذج ربح أخرى. وينبغي للمستخدمين مراجعة سياسة الخصوصية لدى المزوّد وملكيته وعمليات التدقيق ونموذج عمله قبل الاستخدام.

Q7: ما سياسة "عدم الاحتفاظ بالسجلات" (no-logs)؟

تصف سياسة عدم الاحتفاظ بالسجلات أي بيانات نشاط واتصال يقول المزوّد إنه لا يحتفظ بها. ويختلف النطاق الدقيق، لذا ينبغي للقراء مراجعة السياسة ونتائج التدقيق المستقل.

Q8: كيف أختار أفضل VPN؟

ابحث عن سياسات عدم الاحتفاظ بالسجلات المدقَّقة، والبروتوكولات القوية (WireGuard وOpenVPN)، ومواقع الخوادم الآمنة، والسرعات العالية، والخوادم التي تعمل بذاكرة RAM فقط، وميزة مفتاح الإيقاف (kill switch)، وولاية قضائية خارج تحالفات تبادل المعلومات الاستخباراتية (مثل 5/9/14 Eyes).

Q9: هل يمكنني استخدام VPN على هاتفي وتلفازي الذكي؟

نعم. يقدم مزوّدو VPN الحديثون تطبيقات مخصصة لأنظمة iOS وAndroid وmacOS وWindows وLinux والتلفزيونات الذكية، فضلًا عن إعدادات أجهزة التوجيه لحماية جميع الأجهزة في شبكة منزلك.

Q10: ما مفتاح الإيقاف (Kill Switch)؟

مفتاح الإيقاف ميزة أمنية تقطع اتصال جهازك بالإنترنت تلقائيًا إذا انقطع اتصال VPN. وهذا يمنع تسرب بياناتك غير المشفّرة أو عنوان IP الحقيقي.

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

استكشف الجوانب التقنية والبنيوية للشبكات الافتراضية الخاصة وبروتوكولات النفق الآمن.

Q1: ما الفرق بين WireGuard وOpenVPN وIKEv2؟

WireGuard بروتوكول حديث وخفيف (نحو 4,000 سطر من الشيفرة فقط) يوفر سرعات عالية وأوقات اتصال سريعة. أما OpenVPN فهو بروتوكول مفتوح المصدر شديد الأمان ومجرّب ميدانيًا. ويُعد IKEv2 ممتازًا للأجهزة المحمولة لقدرته على إعادة الاتصال بسرعة عند التبديل بين الشبكات. [3]

Q2: ما التوجيه عبر VPN المزدوج أو Multi-Hop؟

يوجّه Multi-Hop حركة مرورك عبر خادمين أو أكثر من خوادم VPN بالتسلسل. ويضيف ذلك طبقة تشفير ثانية ويساعد على إبقاء عنوان IP الحقيقي مخفيًا عن القفزة الثانية إذا اختُرق أحد الخوادم.

Q3: ما تسرب WebRTC وكيف يمنعه VPN؟

WebRTC بروتوكول متصفح قد يكشف عنوانَي IP المحلي والعام الحقيقيين لديك حتى مع تفعيل VPN. وتحجب خدمات VPN المميزة طلبات WebRTC أو تزيّفها في تطبيقات سطح المكتب والجوال وإضافات المتصفح.

Q4: ما الخوادم العاملة بالذاكرة العشوائية فقط ولماذا تهم؟

تكتب الخوادم التقليدية البيانات على أقراص صلبة، يمكن مصادرتها أو اختراقها. أما الخوادم التي تعمل بذاكرة RAM فقط (دون أقراص) فتعمل بالكامل في ذاكرة متطايرة (RAM). وعند إعادة تشغيل الخادم أو إيقاف تشغيله، تُمحى البيانات المحفوظة في الذاكرة.

Q5: كيف تتجاوز التعمية (Obfuscation) حظر VPN؟

يُخفي التعتيم (أو "Stealth VPN") حركة مرور VPN لتبدو كحركة مرور HTTPS عادية (المنفذ 443). وقد يساعدها هذا على تجاوز الفحص العميق للحزم (DPI) الذي تستخدمه الحكومات أو شبكات المدارس والمكاتب لحظر شبكات VPN.

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

استكشف الجوانب التقنية والبنيوية للشبكات الافتراضية الخاصة وبروتوكولات النفق الآمن.

Q6: ما النفق المجزّأ ومتى ينبغي لي استخدامه؟

يتيح لك النفق المقسّم اختيار التطبيقات التي تُوجَّه عبر نفق VPN المشفر وتلك التي تتصل بالإنترنت مباشرة. استخدمه لتوجيه تطبيقات الخدمات المصرفية الحساسة عبر VPN بينما تتصل الألعاب المحلية مباشرة، لتجنب التأخير الذي يضيفه VPN.

Q7: كيف تعمل السرية الأمامية (Perfect Forward Secrecy)؟

تضمن السرية المستمرة الكاملة (PFS) توليد مفتاح تشفير مؤقت فريد لكل جلسة على حدة. وحتى إذا اختُرق مفتاح خاص في المستقبل، فلا يمكن استخدامه لفك تشفير الجلسات السابقة أو اللاحقة لأنها استخدمت مفاتيح مستقلة.

Q8: ما تحالفات العيون 5/9/14 ولماذا ينبغي أن تهمني؟

قد تؤثر الولاية القضائية على الإجراءات القانونية التي قد يواجهها المزوّد، لكن خطر الخصوصية العملي يعتمد أيضًا على البيانات التي يحتفظ بها المزوّد وبنيته التقنية وملكيته وتقارير الشفافية وسجل التدقيق.

Q9: ما الحماية من تسرب DNS؟

تجبر الحماية من تسرّب DNS جهازك على إرسال استعلامات البحث عن المواقع (استعلامات DNS) عبر خوادم DNS الخاصة والمشفّرة التابعة لـ VPN بدلًا من خوادم مزوّد خدمة الإنترنت. وهذا يمنع مزوّد الخدمة من تتبع المواقع التي تزورها.

Q10: هل يمكن لـ VPN تجاوز تقييد سرعة الإنترنت من مزوّد الخدمة؟

أحيانًا. قد يساعد VPN عندما يبطّئ مزوّد خدمة الإنترنت أنشطة معينة يمكن تحديدها، لكنه لن يتغلب على الازدحام أو حدود البيانات أو حدود السرعة على مستوى الحساب أو ضعف جودة الشبكة.

الجزء 11: 10 حقائق مثيرة عن VPN ورؤى من الواقع

راجع هذه الحقائق والرؤى الواقعية القيّمة حول تاريخ شبكات VPN وسوقها وتقنيتها.

1. أول بروتوكول VPN

طُوّر PPTP (بروتوكول النفق من نقطة إلى نقطة) على يد مجموعة من الموردين تضم Microsoft، ونُشر بوصفه RFC 2637 في يوليو 1999 لدعم شبكات VPN للوصول عن بُعد. [6]

2. تقييم السوق

شهد سوق VPN العالمي نموًا سريعًا، مدفوعًا بتزايد متطلبات العمل عن بُعد والاحتياجات الأمنية للمؤسسات.

3. ثورة WireGuard

يتميز WireGuard بشيفرة مبسّطة للغاية مصممة للكفاءة، مما يسهّل تدقيقها بحثًا عن الثغرات الأمنية مقارنة بالبروتوكولات التقليدية. [3]

4. معايير تدقيق صارمة

توظف أبرز مزودي VPN مدققين خارجيين (مثل Cure53 أو PwC) لإجراء مراجعات مستقلة للشيفرة والتحقق من أنهم لا يسجلون أي نشاط للمستخدمين.

5. أصول تحالف Eyes-5

نشأ تحالف Five Eyes من اتفاقية UKUSA لاستخبارات الإشارات عام 1946 بين الولايات المتحدة والمملكة المتحدة، وانضمت إليهما لاحقًا كندا وأستراليا ونيوزيلندا.

6. الفحص العميق للحزم

يفحص الفحص العميق للحزم (DPI) محتويات الحزم وأنماط حركة المرور، لا الترويسات فحسب، وتستخدمه بعض جدران الحماية لرصد بروتوكولات VPN الشائعة وحجبها.

7. الاستخدام المؤسسي

تستخدم نسبة كبيرة من موظفي المؤسسات حول العالم شبكات VPN آمنة لتسجيل الدخول إلى قواعد البيانات الداخلية، مما يجعله معيارًا أمنيًا رئيسيًا.

8. شبكات VPN اللامركزية

تُوزّع شبكات VPN اللامركزية (dVPNs) حركة المرور عبر شبكة من العقد التي يديرها الأقران، ما يقلل الاعتماد على مزوّد مركزي واحد.

9. إخفاء الهوية: TOR مقابل VPN

ينقل VPN الحركة عبر مزوّد واحد، بينما ترسل Tor (The Onion Router) الحركة عبر ثلاث مرحّلات تطوعية (الحارس والوسيط والخروج) بحيث لا تعرف أي مرحّلة واحدة الطرفين معًا.

10. تكلفة اختراقات البيانات

يساعد اعتماد نموذج وصول آمن بمبدأ انعدام الثقة مع VPN المؤسسات على حماية الملكية الفكرية وتخفيف الأثر المالي لاختراقات البيانات.

المراجع والمصادر التقنية

المنشورات المستشهد بها والمواصفات التشفيرية ومعايير الوثائق الرسمية المستخدمة في ورقة العمل هذه.

الأدبيات الأكاديمية والمعايير الأمنية

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

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

ملخص المعايير التقنية

- معايير التغليف: يعرّف RFC 4301 توجيه حزم الإنترنت الآمن لـ IPsec/L2TP.
- تتبع مزوّد خدمة الإنترنت: يمكن أن يقلل توجيه استعلامات DNS عبر نفق VPN المشفر من رؤية مزوّد خدمة الإنترنت المحلي لها.
- بروتوكولات التحكم في جدار الحماية: تتجاوز الحزم المعماة الخفية مرشّحات الحزم العميقة.

مفتاح الإجابة: نقطة التحقق 1 - اختيار من متعدد

1 السؤال 1

الإجابة الصحيحة: **B**

ملاحظة للمعلم

يحدد بروتوكول VPN قواعد بناء النفق وتشفير البيانات؛ أما الخيارات الأخرى فتصف الكابلات وحاجبات الإعلانات ومزوّدي الإنترنت.

2 السؤال 2

الإجابة الصحيحة: **A**

ملاحظة للمعلم

تضيف المسافة زمن تأخر ويملك الخادم المثقل سعة أقل للمشاركة؛ ولا تؤثر دقة الشاشة وملفات تعريف الارتباط وتخطيط لوحة المفاتيح في سرعة الاتصال.

3 السؤال 3

الإجابة الصحيحة: **C**

ملاحظة للمعلم

في الشبكات المفتوحة يمكن للآخرين اعتراض الحزم غير المشفرة؛ ويشفّر VPN الحركة بحيث لا يمكن قراءة البيانات المعترضة.

4 السؤال 4

الإجابة الصحيحة: **B**

ملاحظة للمعلم

يطابق الحجب الجغرافي عنوان IP العام للزائر مع قاعدة بيانات للمواقع ويمنع الوصول خارج المناطق المسموح بها.

5 السؤال 5

الإجابة الصحيحة: **B**

ملاحظة للمعلم

يستطيع مزوّد الإنترنت رؤية أنك ترسل بيانات مشفرة إلى خادم VPN، لكن ليس المواقع التي تزورها أو ما تبحث عنه.

مفتاح الإجابة: نقطة التحقق 2 - صحيح أو خطأ

6 السؤال 6

الإجابة الصحيحة: صحيح

ملاحظة للمعلم

ترى المواقع عنوان IP الخاص بخادم VPN بدلًا من عنوانك، مما يخفي عنها موقعك التقريبي.

7 السؤال 7

الإجابة الصحيحة: خطأ

ملاحظة للمعلم

يقلل التشفير والقفزة الإضافية إلى خادم VPN السرعة قليلًا عادةً؛ ولا يمكن لـ VPN مضاعفة سرعة اتصالك الأساسية.

8 السؤال 8

الإجابة الصحيحة: صحيح

ملاحظة للمعلم

على شبكة Wi-Fi غير مؤمَّنة، يمكن لأدوات اعتراض الحزم التقاط الحركة غير المشفرة مثل بيانات تسجيل الدخول المرسلة دون HTTPS.

9 السؤال 9

الإجابة الصحيحة: صحيح

ملاحظة للمعلم

يمكن للمديرين حظر منافذ VPN المعروفة، مثل المنفذ 1194 في OpenVPN، أو استخدام الفحص العميق للحزم (DPI) لاكتشاف حركة VPN.

10 السؤال 10

الإجابة الصحيحة: خطأ

ملاحظة للمعلم

سياسة عدم الاحتفاظ بالسجلات هي وعد من المزوّد بعدم الاحتفاظ بسجلات نشاطك؛ ولا يوجد قانون يُلزم خدمات VPN بتخزين عمليات البحث لمدة 30 يومًا.

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

H 1. النفقة	A 2. البروتوكول	B 3. النطاق الترددي	E 4. الخادم
C 5. الحظر الجغرافي	D 6. جدار الحماية	F 7. الخصوصية	G 8. مزوّد الإنترنت

نقطة التحقق 3: مفتاح الإجابة – المصطلحات الأساسية

1 التغليف	2 عرض النطاق	3 الجغرافي	4 بروتوكول
5 جدار حماية	6 خادم		

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

1 G – الخصوصية	2 E – الجغرافي	3 B – البروتوكول	4 F – جدارحماية
5 C – عرضالنطاق	6 D – الخادم	7 H – مزودالخدمة	8 A – التغليف

ملاحظات النقاش للمعلمين

المصطلحات الأساسية:
تحقّق من قدرة الطلاب على شرح النفقة والبروتوكول والنطاق الترددي بكلماتهم الخاصة وإعطاء مثال على كل منها.

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

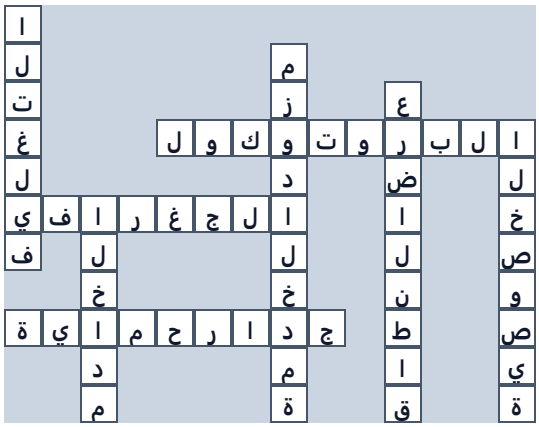
تقييم المصادر:
اطلب من الطلاب التحقق من ادعاء واحد على الأقل من مراجع ورقة العمل، وناقش لماذا قد تتغير الأرقام والأسعار والقواعد مع الوقت.

مفاتيح الألغاز وملاحظات المعلم

حل البحث عن الكلمات

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

حل الكلمات المتقاطعة



أفقي

4 أفقي: البروتوكول مجموعة قواعد تحدد كيفية إرسال البيانات عبر الشبكة (10 حروف)

5 أفقي: الجغرافي قيد يمنع الوصول إلى الويب بحسب الموقع المادي (8 حروف)

7 أفقي: جدارحماية نظام أمان يراقب الحركة غير المصرح بها ويحجبها (9 حروف)

عمودي

1 عمودي: التغليف لف حزم البيانات داخل حزمة أخرى للنقل الآمن (7 حروف)

2 عمودي: مزودالخدمة مزود خدمة الإنترنت الذي يسجل حركتك ما لم تكن مشفرة (10 حروف)

3 عمودي: عرضالنطاق أقصى معدل لنقل البيانات عبر الاتصال (9 حروف)

4 عمودي: الخصوصية حالة التحرر من التتبع أو المراقبة العامة (8 حروف)

6 عمودي: الخادم حاسوب بعيد يوجه حركتك ويخفي عنوان IP الخاص بك (6 حروف)

مفتاح حل الكلمات المبعثرة والشيفرة

مفتاح تصحيح لنشاط فك خلط مفردات المصطلحات وتحدي الشيفرة السرية.

مفتاح ترتيب الكلمات المبعثرة

1. غيالفتل → **التغليف**
2. قعاارنطلض → **عرضالنطاق**
3. غلارايفج → **الجغرافي**
4. صيةصوالخ → **الخصوصية**
5. كتللرورواوب → **البروتوكول**
6. دااخمل → **الخادم**
7. مجيةاردحا → **جدارحماية**
8. مدلةمازخدو → **مزودالخدمة**

مفتاح تحدي الشيفرة السرية

"احم خصوصيتك بنفق آمن"

مفتاح إجابات دراسات الحالة

A السيناريو A: أمان الشبكة العامة

التنصت والتشفير | معضلة سارة

دليل التصحيح

ينبغي أن تغطي إجابات الطلاب النقاط التالية:

- المخاطر: التنصت على الحزم، واعتراض البيانات، وهجمات الوسيط (man-in-the-middle). قد يلتقط شخص على شبكة المقهى نفسها بيانات تسجيل دخولها أو ملف واجبها.
- حماية VPN: تشفّر حمولات حزم الشبكة، مما يجعل حركة النفق المعترَضة غير مقروءة للمتنصتين السلبيين على الشبكة المحلية عند ضبط VPN بشكل صحيح.

B السيناريو B: الوصول إلى الموارد المحظورة

الحجب الجغرافي وعناوين IP | معضلة Alex

دليل التصحيح

ينبغي أن تغطي إجابات الطلاب النقاط التالية:

- سبب الحجب: تستخدم منصة البث الحجب الجغرافي، الذي يربط عنوان IP المحلي للمسافر ببلده الفعلي ويحجبه استنادًا إلى تراخيص الأقاليم.
- كيف يساعد VPN: إخفاء موقعه الحقيقي بتوجيه حركة البيانات عبر خادم في بلده. يرى الموقع عنوان IP لبلده، مما يتيح الوصول.