الاسم: _____ التاريخ: _____ الدرجة: _____

كيف تخفي عنوان IP الخاص بك
ورقة العمل

إخفاء عناوين IP وإخفاء الموقع والوكيل وTor ومنع تسريبات DNS/WebRTC

نظرة تعليمية عامة على VPN

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.

المتعلّم
حالة الطالب
مسار مدافع الشبكات

آمن
حالة الاتصال
حماية حزم البيانات

مُفعّل
الحماية من التسرّب
الحماية من تسرّب DNS وIPv6

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 كيف تعمل عناوين IP وكيف تكشف المواقع.
- قارن بين الوكلاء وTor وشبكات VPN في إخفاء عناوين الشبكة.
- تعرّف على طرق اكتشاف تسريبات DNS وWebRTC ومنعها.
- افهم كيف تتتبع المواقع الإلكترونية المستخدمين عبر عنوان IP العام الخاص بهم.
- قيّم التوجيه متعدد القفزات والأنفاق المشفّرة لحماية IP.

تعليمات ورقة عمل حماية IP

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 إخفاء عنوان IP الخاص بك ومنع التسريبات. واختم بالنشاط الإضافي «فكّر بسرعة».

إخفاء عنوان IP الخاص بك (مقدمة)

عنوان IP الخاص بك هو عنوان بريدي رقمي يكشف موقعك الفعلي وعاداتك على الشبكة. وإخفاء عنوان IP هو خط الدفاع الأول ضد التتبع عبر الإنترنت وبناء ملفات التعريف المستهدفة والحظر الجغرافي. ويساعد فهم كيفية إخفاء عنوانك بأمان على حماية خصوصيتك على الإنترنت.

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

نقطة التحقق 1: تحدي الاختيار من متعدد

1. 1. ماذا يكشف عنوان IP العام للجهاز للمواقع التي تزورها؟
   - A. رقم بطاقة ائتمان المستخدم
   - B. موقعك التقريبي واسم مزوّد الإنترنت لديك
   - C. دليل الملفات المحلي الكامل
   - D. إعدادات لغة لوحة المفاتيح

2. 2. ما الطريقة التي تخفي عنوان IP وتشفّر جميع الحركة على مستوى النظام؟
   - A. وكيل ويب قياسي
   - B. مسح ملفات تعريف الارتباط في متصفحك
   - C. شبكة افتراضية خاصة (VPN)
   - D. تعطيل جدار الحماية الأصلي لديك

3. 3. ما القيد الرئيسي في الخصوصية عند استخدام وكيل ويب مجاني؟
   - A. لا يشفّر حركة البيانات على الشبكات العامة
   - B. يتطلب تثبيت نظام تشغيل خارجي
   - C. غير قانوني تمامًا في الولايات المتحدة
   - D. يتطلب اتصال خط هاتف مخصصًا

4. 4. كيف توفر شبكة Tor إخفاءً عاليًا للهوية للمستخدمين؟
   - A. بتسريع سرعات الاتصال
   - B. بتوجيه الحركة عبر ثلاثة مرحّلات يديرها متطوعون
   - C. بتسجيل اسمك في قاعدة بيانات عالمية
   - D. بقصر الوصول على الجهات الحكومية فقط

5. 5. ما هو تسريب DNS؟
   - A. خطأ في إرسال بريد إلكتروني إلى عنوان خاطئ
   - B. عندما تتجاوز استعلامات DNS نفق VPN وتذهب إلى مزود خدمة الإنترنت
   - C. عطل في العتاد بمصدر طاقة الموجّه المحلي
   - D. تحديث لبرنامج تشغيل محول الشبكة المحلية

نقطة التحقق 2: تحدي صحيح أم خطأ

6 سؤال 6

6. يشفّر خادم الوكيل حركة نظام التشغيل في الخلفية تمامًا مثل VPN.

○ صحيح ○ خطأ

7 سؤال 7

7. توجيه Tor آمن للغاية لكنه يقلل سرعة تصفح الشبكة.

○ صحيح ○ خطأ

8 سؤال 8

8. قد تكشف تسريبات WebRTC عنوان IP الحقيقي لديك أثناء جلسة VPN نشطة.

○ صحيح ○ خطأ

9 سؤال 9

9. مع تشغيل VPN وبدون تسريبات، لا يستطيع مزوّد الإنترنت رؤية المواقع التي تزورها.

○ صحيح ○ خطأ

10 سؤال 10

10. يمنع إخفاء عنوان IP الخاص بك التتبع عبر بصمة المتصفح.

○ صحيح ○ خطأ

نقطة التحقق 3: إدراج المصطلحات الأساسية

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

1. يسمى التجاوز الذي يكشف استعلامات نطاقك لنفق آمن _____ .
2. قد تسرب واجهات برمجة اتصالات _____ المعتمدة على المتصفح عنوان IP الأصلي لجهازك.
3. يعيد _____ الويب توجيه حركة المتصفح لكنه لا يشفر حمولة الحزم.
4. يوفر التشفير متعدد الطبقات في شبكة _____ مستويات عالية من إخفاء الهوية.
5. يخصص لك مزود الاتصالات _____ العام الذي يكشف منطقتك.
6. يتحقق تجاوز الحجب الإقليمي للوسائط عبر تمويه _____ .

بنك كلمات المفردات

التتبع | الموقع | النفق | تسريب DNS | تور | عنوان IP | وكيل | WebRTC

اكتب إجاباتك هنا:

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

نقطة التحقق 4: مطابقة مفاهيم الشبكات

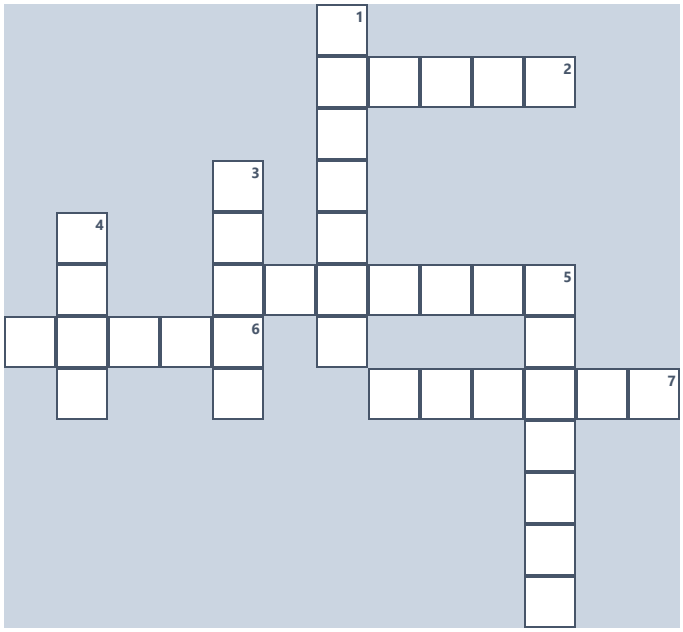
مطابقة التعريفات

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

1. عنوان IP	A	يشفّر كل حركة الجهاز ويوجهها عبر خادم VPN.
2. نفق VPN	B	يمرر البيانات عبر ثلاثة خوادم متطوعة، مع تشفير الطبقات في كل خطوة.
3. شبكة Tor	C	توجيه الاتصال عبر خادم في بلد آخر لتجاوز الحظر الجغرافي.
4. وكيل الويب	D	تسمية رقمية فريدة تحدد واجهة جهاز على الإنترنت.
5. تسريب DNS	E	يعيد توجيه حركة المتصفح على طبقة التطبيقات دون تشفير على مستوى النظام.
6. واجهة WebRTC البرمجية	F	تسجيل وجهات حركة الإنترنت غير المشفرة بواسطة شركة الاتصالات لديك.
7. إخفاء الموقع	G	استعلامات تُحلَّل خارج نفق VPN، مما يكشف النطاقات التي تمت زيارتها لمزوّد خدمة الإنترنت.
8. تتبع مزوّد الإنترنت	H	ميزة في المتصفح للصوت/الفيديو يمكنها تجاوز الأنفاق وكشف عناوين IP الحقيقية.

نقطة التحقق 5: لغز الكلمات المتقاطعة

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



أفقي

2. استعلامات تحل خارج نفق VPN فتكشف النطاقات المزارة لمزود الإنترنت (5)

5. معرف رقمي فريد لواجهة جهاز على الإنترنت (7)

6. ميزة متصفح للصوت والفيديو (WebRTC) قد تتجاوز الأنفاق وتكشف عناوين IP الحقيقية (5)

7. تسجيل وجهات حركة الإنترنت غير المشفرة بواسطة شركة الاتصالات (6)

عمودي

1. توجه البيانات عبر ثلاثة خوادم متطوعة مع تشفير الطبقات في كل خطوة (7)

3. يشفر كل حركة الجهاز ويوجهها عبر خادم VPN (5)

4. يعيد توجيه حركة المتصفح على مستوى التطبيق دون تشفير على مستوى النظام (4)

5. توجيه الاتصال عبر خادم في بلد آخر لتجاوز الحجب الجغرافي (7)

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

2 أفقي: استعلامات تحل خارج نفق VPN فتكشف النطاقات المزارة لمزود الإنترنت (5 حروف):

5 أفقي: معرف رقمي فريد لواجهة جهاز على الإنترنت (7 حروف):

6 أفقي: ميزة متصفح للصوت والفيديو (WebRTC) قد تتجاوز الأنفاق وتكشف عناوين IP الحقيقية (5 حروف):

7 أفقي: تسجيل وجهات حركة الإنترنت غير المشفرة بواسطة شركة الاتصالات (6 حروف):

عمودي

1 عمودي: توجه البيانات عبر ثلاثة خوادم متطوعة مع تشفير الطبقات في كل خطوة (7 حروف):

3 عمودي: يشفر كل حركة الجهاز ويوجهها عبر خادم VPN (5 حروف):

4 عمودي: يعيد توجيه حركة المتصفح على مستوى التطبيق دون تشفير على مستوى النظام (4 حروف):

5 عمودي: توجيه الاتصال عبر خادم في بلد آخر لتجاوز الحجب الجغرافي (7 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.

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

قائمة كلمات المفردات

العنوان
النفق
شبكةتور
وكيل
تسريب
فورية
التمويه
التتبع

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. العنوان
B. النفق
C. شبكةتور
D. وكيل
E. تسريب
F. فورية
G. التمويه
H. التتبع

التعريفات وحقول المطابقة
1. يعيد توجيه حركة المتصفح على مستوى التطبيق دون تشفير على مستوى النظام.
2. توجيه الاتصال عبر خادم في بلد آخر لتجاوز الحجب الجغرافي.
3. ميزة متصفح للصوت والفيديو (WebRTC) قد تتجاوز الأنفاق وتكشف عناوين IP الحقيقية.
4. معرف رقمي فريد لواجهة جهاز على الإنترنت.
5. توجه البيانات عبر ثلاثة خوادم متطوعة مع تشفير الطبقات في كل خطوة.
6. تسجيل وجهات حركة الإنترنت غير المشفرة بواسطة شركة الاتصالات.
7. استعلامات تحل خارج نفق VPN فتكشف النطاقات المزارة لمزود الإنترنت.
8. يشفر كل حركة الجهاز ويوجهها عبر خادم VPN.

نقطة التحقق 7: تحدي الكلمات المبعثرة

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

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

نشاط إضافي: فكّر بسرعة

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

1	أسباب لاستخدام VPN أثناء السفر		
2	متصفحات تعرفها		
3	أشياء يمكن أن يخفيها VPN		
4	كلمات متعلقة بالخصوصية		
5	كلمات من ورقة العمل هذه تريد تذكّرها		
6	أشياء يمكن للموقع تخمينها من عنوان IP الخاص بك		
7	أرقام أو رموز في عنوان IP		
8	خرافات عن VPN		
9	خدمات VPN التي تعرفها		
10	أشياء يستطيع مزوّد الإنترنت رؤيتها		
11	وعود يقدمها مزوّد VPN جيد		
12	أشياء قد تسرّب عنوان IP الحقيقي الخاص بك		
13	أسباب لإخفاء موقعك		
14	طرق لإخفاء عنوان IP الخاص بك		
15	أجهزة يمكنها استخدام VPN		

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

لإكمال تدريبك على إخفاء IP، فك تشفير هذه الرسالة السرية عن إخفاء آثارك الرقمية.

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

1	7	20		18	25	27	1	25	22		2	25	17	1	24		7	20	28

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 يخفي الوكيل عبر الويب (web proxy) عنوان IP الخاص بي؟

نعم، لكن فقط للحركة المرسلة عبره، وهي عادةً حركة متصفحك. ولا تشفّر معظم وكلاء الويب بياناتك، لذا قد يظل مزود خدمة الإنترنت أو مشغّل الشبكة قادرًا على رؤية ما ترسله وتستقبله.

Q5: هل إخفاء عنوان IP الخاص بي قانوني؟

في بلدان كثيرة نعم، لكن بعضها يقيّد VPN وغيره من أدوات إخفاء عنوان IP أو يحظرها. ولا يجعل إخفاء عنوان IP الخاص بك أي فعل غير قانوني قانونيًا، لذا تحقق من القوانين المحلية قبل استخدامه.

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 يخفي Tor عنوان IP الخاص بي؟

نعم. ترسل Tor حركة بياناتك عبر ثلاث مرحلات متطوعة (الحارس والوسيط والخروج)، فترى المواقع عنوان مرحّل الخروج، ولا يعرف أي مرحّل بمفرده من أنت وإلى أين تذهب. [1]

Q7: ماذا يكشف عنوان IP الخاص بي؟

يكشف عنوان IP العام الخاص بك عادةً مزوّد خدمة الإنترنت وموقعًا تقريبيًا، مثل بلدك أو مدينتك. ويمكن للمواقع أيضًا استخدامه لربط زياراتك معًا ولتطبيق الحظر الجغرافي.

Q8: كيف أتحقق من أنه مخفي؟

اتصل بـ VPN، ثم زر موقعًا لفحص IP وشغّل اختبارات تسرب DNS وWebRTC. يجب أن ينتمي عنوان IP وخوادم DNS الظاهرة إلى VPN، لا إلى مزود الإنترنت لديك. وإذا ظهر عنوان IP الحقيقي لديك، ففعّل حماية التسرب.

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: لماذا لا تزال المواقع قادرة على تتبعي بعد إخفاء عنوان IP؟

لا يمنع إخفاء عنوان IP الخاص بك بصمة المتصفح. يمكن للمتتبعات دمج تفاصيل مثل دقة الشاشة والخطوط المثبتة وإعدادات المتصفح في معرّف واحد، كما يمكن لملفات تعريف الارتباط أو الحسابات المسجَّل دخولها أن تحدد هويتك أيضًا، لذا استخدم متصفحًا يركز على الخصوصية كذلك. [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: هل يمكن لحركة IPv6 أن تسرّب عنوان IP الحقيقي الخاص بي؟

نعم، إذا كان VPN لديك ينقل IPv4 فقط عبر النفق. فقد يرسل جهازك حينئذٍ حركة IPv6 خارج النفق، فيكشف عنوانًا مُعيّنًا من مزوّد خدمة الإنترنت. استخدم VPN ينقل IPv6 عبر النفق أو يحظره، وتأكد من ذلك باختبار تسرّب IPv6.

Q5: كيف تتجاوز التعمية (Obfuscation) حظر VPN؟

يُخفي التعتيم (أو "Stealth VPN") حزم حركة مرور VPN لتبدو كحركة مرور ويب HTTPS عادية (المنفذ 443). وهذا يساعد 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: هل يكشف النفق المجزّأ عنوان IP الحقيقي الخاص بي؟

نعم، بالنسبة إلى التطبيقات التي تستثنيها. تستخدم حركة البيانات المرسلة خارج النفق عنوان IP الحقيقي لديك، وتشير RFC 8828 إلى أن WebRTC قد يكشف عنوان مزوّد خدمة الإنترنت أسفل VPN بنفق مقسّم ما لم يقيّده المتصفح. [2]

Q7: ما عنوان IP المشترك وكيف يفيد الخصوصية؟

مع عنوان IP مشترك، يظهر كثير من مستخدمي VPN متصلين بالعنوان نفسه في الوقت نفسه. وهذا يجعل ربط موقع ما أي زيارة منفردة بك أصعب بكثير مقارنة بعنوان IP مخصص يستخدمه أنت فقط.

Q8: هل يستطيع مزوّد خدمة الإنترنت رؤية أنني أستخدم VPN لإخفاء عنوان IP؟

عادةً نعم. يستطيع مزود خدمة الإنترنت لديك أن يرى أنك تتصل بعنوان IP لخادم VPN، ووقت اتصالك، وحجم البيانات التي ترسلها، لكنه لا يرى المواقع التي تزورها ولا المحتوى داخل النفق المشفر.

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: أيهما أفضل لإخفاء عنوان IP: الوكيل أم VPN؟

VPN هو الأفضل عادةً. فهو يخفي IP الخاص بك لكل تطبيق على الجهاز ويشفّر الحركة، بينما يغطي الوكيل عبر الويب المتصفح عادةً فقط وغالبًا لا يضيف أي تشفير.

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

يُعد PPTP (بروتوكول النفق من نقطة إلى نقطة)، وهو بروتوكول VPN مبكر من مجموعة تقودها Microsoft في عقد 1990، غير آمن الآن، لذا تستخدم شبكات VPN الحديثة WireGuard أو OpenVPN.

2. أخذ البصمة

لا يمنع إخفاء عنوان IP الخاص بك بصمة المتصفح، التي يمكنها تحديد هويتك من تفاصيل مثل دقة الشاشة والخطوط المثبتة. [3]

3. ثورة WireGuard

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

4. كشف عنوان WebRTC

يحذّر RFC 8828 من أن WebRTC قد يكشف كلًا من العنوان العام لشبكة VPN وعنوان مزوّد خدمة الإنترنت الذي يعمل VPN فوقه، ما لم يقيّده المتصفح. [2]

5. أصول تحالف Eyes-5

نشأت شراكة Five Eyes الاستخباراتية بين الولايات المتحدة والمملكة المتحدة وكندا وأستراليا ونيوزيلندا من التعاون في استخبارات الإشارات بين الحلفاء في عهد الحرب العالمية الثانية.

6. الفحص العميق للحزم

تنشر جدران الحماية المتقدمة الفحص العميق للحزم (DPI) لتحليل بيانات الحزم الوصفية وحظر خصائص اتصال VPN القياسية.

7. إعادة استخدام دائرة TOR

يعيد Tor استخدام الدائرة نفسها نحو عشر دقائق ثم يبني دائرة جديدة، مما يصعّب ربط أنشطة تصفحك ببعضها. [1]

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) لتعظيم الخصوصية. [1]

10. الوكلاء مقابل أنفاق VPN

يغيّر وكيل الويب عنوان IP الذي يراه الموقع لحركة متصفحك، لكنه بخلاف VPN لا يشفّر عادةً تلك الحركة ولا يغطي التطبيقات الأخرى على جهازك. [5]

المراجع والمصادر التقنية

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

المراجع الأكاديمية والصناعية

[1] Tor Project. (n.d.). Overview.
https://support.torproject.org/about-tor/how-tor-works/overview/

[2] IETF. (2021). RFC 8828: WebRTC IP Address Handling Requirements.
https://www.rfc-editor.org/rfc/rfc8828

[3] Electronic Frontier Foundation. (n.d.). Cover Your Tracks: Learn.
https://coveryourtracks.eff.org/learn

[4] Electronic Frontier Foundation. (2026). Choosing the VPN That's Right for You.
https://ssd.eff.org/module/choosing-vpn-thats-right-you

[5] Federal Trade Commission. (2018). FTC Provides Tips for Using VPN Apps.
https://www.ftc.gov/news-events/news/press-releases/2018/02/ftc-provides-tips-using-vpn-apps

مفتاح الإجابة: إخفاء عناوين IP وتمويه الموقع والخادم الوكيل وTor ومنع تسريبات DNS/WebRTC

1 السؤال 1

الإجابة الصحيحة: B

ملاحظة للمعلم

ماذا يكشف عنوان IP العام للجهاز للمواقع التي تزورها؟ ← موقعك التقريبي واسم مزوّد الإنترنت لديك

2 تشفير نظام VPN

زمن الاستجابة

الإجابة الصحيحة: C

ملاحظة للمعلم

بخلاف الوكلاء التي تعيد توجيه حركة المتصفح فقط، ينشئ VPN نفقًا مشفرًا على مستوى النظام كله، فيؤمّن التطبيقات الخلفية والألعاب واستعلامات نظام التشغيل. المرجع: Tor Project Relays, W3C WebRTC API.

3 غياب تشفير الوكيل

أمان Wi-Fi

الإجابة الصحيحة: A

ملاحظة للمعلم

تعيد وكلاء الويب توجيه حركة المتصفح فقط دون تشفير حمولات الحزم، مما يعني أن مشغّل شبكتك أو مزود خدمة الإنترنت لديك قد يتتبع حركة محتواك. الاستشهاد: IETF Proxy Vulnerabilities.

4 السؤال 4

الإجابة الصحيحة: B

ملاحظة للمعلم

كيف توفر شبكة Tor إخفاءً عاليًا للهوية للمستخدمين؟ ← بتوجيه الحركة عبر ثلاثة مرحّلات يديرها متطوعون

5 تسرّبات نفق DNS

الخصوصية

الإجابة الصحيحة: B

ملاحظة للمعلم

يحدث تسرب DNS عندما تتجاوز طلبات حل أسماء النطاقات نفق VPN وتذهب مباشرة إلى محللات مزوّد الإنترنت لديك، فتكشف سجلات النطاقات التي زرتها. المصدر: DNSSEC Tunnel Testing، EFF Tracking Evasion.

مفتاح الإجابة: نقطة التحقق 2 - صحيح أو خطأ

6 تفاصيل قيود الوكيل — إخفاء IP

الإجابة الصحيحة: خطأ

ملاحظة للمعلم

تعمل الوكلاء على طبقة التطبيق وتفتقر إلى تكامل برنامج تشغيل الشبكة على مستوى النظام الذي يتمتع به نفق VPN. المرجع: IETF Proxy Vulnerabilities.

7 السؤال 7

الإجابة الصحيحة: صحيح

ملاحظة للمعلم

يضيف ترحيل الحركة عبر ثلاثة مرحّلات يديرها متطوعون مع تشفير متعدد الطبقات زمن تأخر، لذا يكون Tor أبطأ عادةً من الاتصال المباشر.

8 السؤال 8

الإجابة الصحيحة: صحيح

ملاحظة للمعلم

يمكن لـ WebRTC كشف العناوين المحلية، ومع بعض إعدادات VPN، عنوان IP العام الذي يخصصه مزوّد الإنترنت أسفل النفق (RFC 8828).

9 السؤال 9

الإجابة الصحيحة: صحيح

ملاحظة للمعلم

بدون تسريبات DNS أو WebRTC، لا يرى مزوّد الإنترنت سوى حركة مشفرة إلى خادم VPN، وليس المواقع التي تزورها.

10 حدود البصمة الرقمية — بلا سجلات

الإجابة الصحيحة: خطأ

ملاحظة للمعلم

تستهدف البصمة الرقمية مقاييس إعداد الجهاز (دقة الشاشة والخطوط والإضافات) التي تبقى مرئية حتى عند إخفاء IP. المصدر: EFF Tracking Evasion.

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

D 1. عنوان IP	A 2. نفق VPN	B 3. شبكة Tor	E 4. وكيل الويب
G 5. تسريب DNS	H 6. واجهة WebRTC البرمجية	C 7. إخفاء الموقع	F 8. تتبع مزوّد الإنترنت

نقطة التحقق 3: مفتاح الإجابة – المصطلحات الأساسية

1 تسريب DNS	2 WebRTC	3 وكيل	4 تور
5 عنوان IP	6 الموقع		

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

1 D – وكيل	2 G – التمويه	3 F – فورية	4 A – العنوان
5 C – شبكةتور	6 H – التتبع	7 E – تسريب	8 B – النفق

ملاحظات النقاش للمعلمين

المصطلحات الأساسية:
تحقّق من قدرة الطلاب على شرح عنوان IP ونفق VPN وشبكة Tor بكلماتهم الخاصة وإعطاء مثال على كل منها.

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

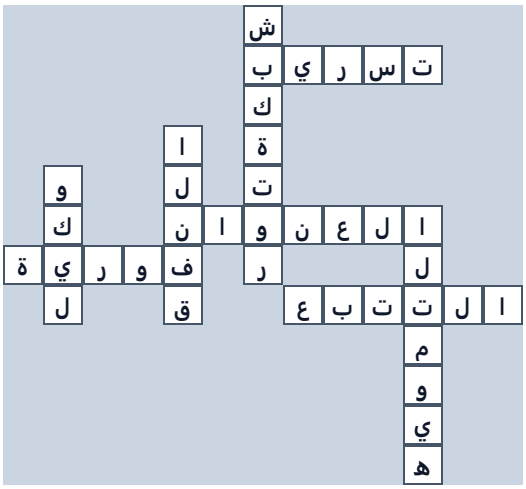
تقييم المصادر:
اطلب من الطلاب التحقق من ادعاء واحد على الأقل من مراجع ورقة العمل، وناقش لماذا قد تتغير الأرقام والأسعار والقواعد مع الوقت.

مفاتيح الألغاز وملاحظات المعلم

حل البحث عن الكلمات

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

حل الكلمات المتقاطعة



دليل المعلم لحلول الكلمات المتقاطعة

أفقي

2 أفقي: تسريب استعلامات تحل خارج نفق VPN فتكشف النطاقات المزارة لمزود الإنترنت (5 حروف)

5 أفقي: العنوان معرف رقمي فريد لواجهة جهاز على الإنترنت (7 حروف)

6 أفقي: فورية ميزة متصفح للصوت والفيديو (WebRTC) قد تتجاوز الأنفاق وتكشف عناوين IP الحقيقية (5 حروف)

7 أفقي: التتبع تسجيل وجهات حركة الإنترنت غير المشفرة بواسطة شركة الاتصالات (6 حروف)

عمودي

1 عمودي: شبكةتور توجه البيانات عبر ثلاثة خوادم متطوعة مع تشفير الطبقات في كل خطوة (7 حروف)

3 عمودي: النفق يشفر كل حركة الجهاز ويوجهها عبر خادم VPN (5 حروف)

4 عمودي: وكيل يعيد توجيه حركة المتصفح على مستوى التطبيق دون تشفير على مستوى النظام (4 حروف)

5 عمودي: التمويه توجيه الاتصال عبر خادم في بلد آخر لتجاوز الحجب الجغرافي (7 حروف)

مفتاح حل الكلمات المبعثرة والشيفرة

مفتاح تصحيح لنشاط فك خلط مفردات المصطلحات وتحدي الشيفرة السرية.

مفتاح ترتيب الكلمات المبعثرة

1. نااونعل — العنوان
2. شكروتةب — شبكةتور
3. رتبيس — تسريب
4. هلوميات — التمويه
5. نقافل — النفق
6. يلوك — وكيل
7. يةفرو — فورية
8. تعابتل — التتبع

مفتاح تحدي الشيفرة السرية

"أخف عنوانك بنظام خفي"

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.