الاسم: _____ التاريخ: _____ الدرجة: _____

WireGuard مقابل OpenVPN
ورقة العمل

مقارنة بروتوكولي WireGuard وOpenVPN وأحجام شيفرتيهما المصدرية وسرعتيهما والمعايير التشفيرية فيهما

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

- قارن تعقيد الشيفرة المصدرية وسرعة تدقيق البروتوكولات.
- حلّل مكاسب الأداء عند التشغيل داخل فضاء النواة.
- قارن شيفرات OpenSSL بالتشفير الحديث في WireGuard.
- إعداد أزواج المفاتيح العامة والخاصة لمصافحات الأقران.
- تمرير حركة VPN عبر منافذ جدار الحماية TCP وUDP.

تعليمات ورقة عمل مقارنة البروتوكولات

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 تدقيق البروتوكولات الحديثة. واختم بالنشاط الإضافي «فكّر بسرعة».

WIREGUARD مقابل OPENVPN (مقدمة)

يتطلب اختيار بروتوكول VPN الموازنة بين السرعة وخيارات الإعداد. ظل OpenVPN المعيار لعقود، إذ يوفر مرونة في إعدادات TCP/UDP. أما WireGuard فهو بديل حديث يعمل مباشرة في فضاء النواة بنحو 4,000 سطر برمجي فقط. وفهم الفروق بين البروتوكولات مفتاح لتحسين شبكاتك الآمنة.

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

نقطة التحقق 1: تحدي الاختيار من متعدد

1. ما الحجم التقريبي للشيفرة المصدرية لبروتوكول WireGuard؟
   - A. نحو 70,000 سطر
   - B. أكثر من 100,000 سطر
   - C. أقل من 1,000 سطر
   - D. نحو 4,000 سطر

2. في أي مساحة من نظام التشغيل يعمل WireGuard؟
   - A. فضاء المستخدم
   - B. فضاء النواة
   - C. فضاء التطبيق
   - D. مساحة افتراضية

3. على أي مكتبة تشفير يعتمد OpenVPN بالدرجة الأولى؟
   - A. ChaCha20-Poly1305
   - B. مكتبة التشفير OpenSSL
   - C. إطار بروتوكول Noise
   - D. ترميز DES كنص صريح

4. ما الميزة الرئيسية في الأداء لـ WireGuard مقارنة بـ OpenVPN؟
   - A. مصافحات اتصال أسرع وزمن استجابة أقل
   - B. تجاوز الحاجة إلى عناوين IP عامة
   - C. دعم أصلي مدمج للاتصال الهاتفي القديم
   - D. حمل إضافي صفري على البطارية في الأجهزة المحمولة

5. كيف يوثّق WireGuard اتصالات النظراء؟
   - A. بتبادل كلمات مرور المستخدمين العادية
   - B. بالتحقق من شهادات تسجيل النطاق
   - C. باستخدام أزواج مفاتيح عامة وخاصة ثابتة
   - D. بفحص الأرقام التسلسلية للعتاد

نقطة التحقق 2: تحدي صحيح أم خطأ

6 سؤال 6

6. شيفرة WireGuard المدمجة تجعل تدقيقه أسهل بكثير.

صحيح خطأ

7 سؤال 7

7. OpenVPN أسرع عمومًا من WireGuard لأنه يعمل في فضاء النواة.

صحيح خطأ

8 سؤال 8

8. OpenVPN قابل للتهيئة بدرجة عالية ويدعم بروتوكولي UDP وTCP.

صحيح خطأ

9 سؤال 9

9. يستخدم WireGuard تشفيرًا حديثًا مثل ChaCha20 لتشفير الحزم بسرعة.

صحيح خطأ

10 سؤال 10

10. يتطلب WireGuard إعدادات معقدة لسلطة الشهادات للمصادقة.

صحيح خطأ

نقطة التحقق 3: إدراج المصطلحات الأساسية

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

1. يعمل بروتوكول _____ الحديث مباشرة داخل نواة نظام التشغيل.
2. يعتمد البروتوكول القديم _____ على مكتبة التشفير OpenSSL.
3. يقلل تنفيذ الشفرة في فضاء _____ عبء تبديل السياق.
4. يعمل OpenVPN في فضاء _____ ويوجه الحزم عبر واجهات افتراضية.
5. يستخدم WireGuard أزواج _____ عامة وخاصة لتعريف أقران الاتصال.
6. يعزز صغر حجم الشفرة قابلية _____ الأمني للبرمجيات.

بنك كلمات المفردات

التدقيق | المستخدم | المفاتيح | المكتبة | النواة | أوبن | وايرغارد | OpenVPN

اكتب إجاباتك هنا:

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

نقطة التحقق 4: مطابقة مفاهيم الشبكات

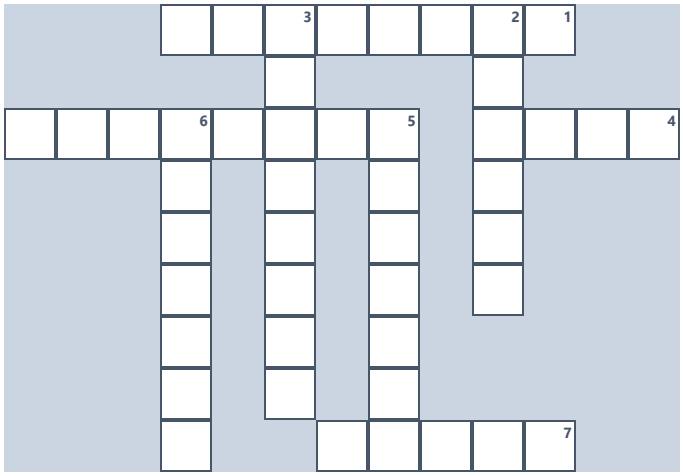
مطابقة التعريفات

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

1. WireGuard	A	منطقة التنفيذ التي يعمل فيها OpenVPN، ما يخلق عبء تبديل السياق.
2. OpenVPN	B	الحجم المضغوط لقاعدة شيفرة WireGuard، مما يجعل تدقيقها أسهل بكثير.
3. فضاء النواة	C	مكتبة تشفيرية يعتمد عليها OpenVPN لخوارزميات الشيفرة.
4. فضاء المستخدم	D	بروتوكولات النقل التي يدعمها OpenVPN؛ بينما يعمل WireGuard نفسه عبر UDP فقط.
5. 4,000 سطر	E	منطقة تنفيذ نظام التشغيل التي يعمل فيها WireGuard لتحقيق السرعة.
6. OpenSSL	F	رموز غير متماثلة يستخدمها WireGuard للتحقق من اتصالات الأقران.
7. زوج المفاتيح	G	بروتوكول VPN حديث مصمم للسرعة العالية وسهولة تدقيق الشيفرة.
8. TCP/UDP	H	بروتوكول قديم متين يستخدم قاعدة شيفرة إعدادات كبيرة ومعقدة.

نقطة التحقق 5: لغز الكلمات المتقاطعة

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



أفقي

1. بروتوكول VPN حديث مصمم للسرعة العالية وسهولة تدقيق الشفرة (8)

4. بروتوكول قديم متين بقاعدة شفرة كبيرة وإعدادات معقدة (4)

5. رموز غير متماثلة يستخدمها WireGuard للتحقق من اتصالات الأقران (8)

7. بروتوكولات نقل يدعمها OpenVPN؛ أما WireGuard فيعمل فوق UDP فقط (5)

عمودي

2. منطقة تنفيذ نظام التشغيل التي يعمل فيها WireGuard طلبا للسرعة (6)

3. منطقة التنفيذ التي يعمل فيها OpenVPN مما يخلق عبء تبديل السياق (8)

5. حجم قاعدة شفرة WireGuard المدمج الذي يجعل مراجعتها أسهل بكثير (7)

6. مكتبة تشفير يعتمد عليها OpenVPN لخوارزميات الشفرات (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

1 أفقي: بروتوكول VPN حديث مصمم للسرعة العالية وسهولة تدقيق الشفرة (8 حروف):

4 أفقي: بروتوكول قديم متين بقاعدة شفرة كبيرة وإعدادات معقدة (4 حروف):

5 أفقي: رموز غير متماثلة يستخدمها WireGuard للتحقق من اتصالات الأقران (8 حروف):

7 أفقي: بروتوكولات نقل يدعمها OpenVPN؛ أما WireGuard فيعمل فوق UDP فقط (5 حروف):

عمودي

2 عمودي: منطقة تنفيذ نظام التشغيل التي يعمل فيها WireGuard طلبا للسرعة (6 حروف):

3 عمودي: منطقة التنفيذ التي يعمل فيها OpenVPN مما يخلق عبء تبديل السياق (8 حروف):

5 عمودي: حجم قاعدة شفرة WireGuard المدمج الذي يجعل مراجعتها أسهل بكثير (7 حروف):

6 عمودي: مكتبة تشفير يعتمد عليها OpenVPN لخوارزميات الشفرات (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.

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

قائمة كلمات المفردات

وايرغارد اوبن النواة المستخدم التدقيق المكتبة المفاتيح النقل

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. وايرغارد
B. اوبن
C. النواة
D. المستخدم
E. التدقيق
F. المكتبة
G. المفاتيح
H. النقل

التعريفات وحقول المطابقة
1. مكتبة تشفير يعتمد عليها OpenVPN لخوارزميات الشفرات.
2. منطقة تنفيذ نظام التشغيل التي يعمل فيها WireGuard طلبا للسرعة.
3. بروتوكول قديم متين بقاعدة شفرة كبيرة وإعدادات معقدة.
4. رموز غير متماثلة يستخدمها WireGuard للتحقق من اتصالات الأقران.
5. بروتوكولات نقل يدعمها OpenVPN؛ أما WireGuard فيعمل فوق UDP فقط.
6. حجم قاعدة شفرة WireGuard المدمج الذي يجعل مراجعتها أسهل بكثير.
7. بروتوكول VPN حديث مصمم للسرعة العالية وسهولة تدقيق الشفرة.
8. منطقة التنفيذ التي يعمل فيها OpenVPN مما يخلق عبء تبديل السياق.

نقطة التحقق 7: تحدي الكلمات المبعثرة

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

1. ررغوادي
2. ةناول
3. داقةتيل
4. فيحتاالم
5. نابو
6. دمسخاتلم
7. ابتةلكم
8. لانقل

نشاط إضافي: فكّر بسرعة

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

1. أسباب لاختيار WireGuard
2. وعود يقدمها مزوّد VPN جيد
3. أسباب لاختيار OpenVPN
4. أسباب لاستخدام VPN أثناء السفر
5. أشياء يستطيع مزوّد الإنترنت رؤيتها
6. طرق لاكتشاف شبكة Wi-Fi مزيفة
7. خرافات عن VPN
8. أماكن تستخدم فيها VPN
9. أشياء سريعة في الحياة اليومية
10. أشياء لا يحميك منها VPN
11. أشياء تجعل فحص الشيفرة البرمجية أسهل
12. أشياء يمكن أن يخفيها VPN
13. فروق بين WireGuard وOpenVPN
14. كلمات متعلقة بالخصوصية
15. أسماء تشفير تعرفها

نقطة التحقق 8: دراسات حالة في VPN

طبّق المفاهيم التي تعلمتها لحل السيناريوهات الواقعية أدناه.

سارة (طالبة المقهى)

👩‍💻 "مرحبًا! أنا على شبكة Wi-Fi في المقهى، ويتيح لي تطبيق VPN لدي اختيار WireGuard أو OpenVPN. تنقطع مكالمات الفيديو لدي باستمرار عندما أتنقل بين شبكة المقهى ونقطة اتصال هاتفي. أي بروتوكول ينبغي أن أختار، ولماذا سيتعامل مع هذا التبديل بصورة أفضل؟"

ALEX (طالب مسافر)

👨‍💻 "أنا في الخارج على شبكة فندق يبدو أنها تحظر معظم حركة VPN. لا يتصل WireGuard إطلاقًا، لكنني أحتاج إلى الوصول إلى موارد مدرستي في بلدي. ما الذي يُرجَّح أنه محظور، وكيف يمكن لـ OpenVPN مساعدتي في تجاوز ذلك؟"

نقطة التحقق 9: فك الشيفرة

لإكمال تدريبك على تدقيق البروتوكولات، فك تشفير هذه الرسالة المخفية عن التنفيذ في فضاء النواة.

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 ه=26 و=27 ي=28 ة=29 ى=30 ء=31 ؤ=32 ئ=33

24	28	8	21	23	1		22	23	1	14	3	1		10	27	16

18	10	12	1		21	20	25	2

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 تهم البروتوكولات؟

يحدد البروتوكول كيف يبني VPN نفقه، وأي تشفير يحمي بياناتك، ومدى سرعة اتصاله وإعادة اتصاله. وWireGuard وOpenVPN هما بروتوكولا المصدر المفتوح اللذان تقدمهما معظم تطبيقات VPN، ولكل منهما مفاضلات مختلفة بين البساطة والسرعة وقابلية الضبط.

Q3: هل أحدهما أكثر خصوصية من الآخر؟

لا يجعلك أي من البروتوكولين مجهولًا. كلاهما يشفّر حركة مرور النفق بشيفرات قوية؛ وتعتمد خصوصيتك في الغالب على ما يسجله مزود VPN وكيفية إدارته للمفاتيح والحسابات والخوادم.

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 كلاهما مفتوح المصدر؟

نعم. ينشر كل من WireGuard والإصدار المجتمعي من OpenVPN شيفرته المصدرية، فيستطيع باحثون مستقلون مراجعتهما. ويجعل صغر شيفرة WireGuard المراجعة الكاملة أسرع بكثير.

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

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

Q6: أيهما أسرع؟

WireGuard عادةً أسرع: فهو يعمل في النواة، ويستخدم تشفير ChaCha20-Poly1305 الخفيف، ويُكمل المصافحات بسرعة. أما OpenVPN فعبئه أكبر، لكن السرعات الفعلية تعتمد أيضًا على حمل الخادم والمسافة.

Q7: هل يمكن لكليهما العمل عبر TCP وUDP؟

لا. فيمكن تشغيل OpenVPN عبر UDP أو TCP، ويفيد وضع TCP على الشبكات التي تحظر UDP. أما WireGuard فيرسل حزمه عبر UDP فقط، لذا قد يفشل على الشبكات التي تسمح بـ TCP فقط. [4]

Q8: كيف أختار أفضل VPN؟

ابحث عن سياسات عدم الاحتفاظ بالسجلات المدقّقة، 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 WireGuard وOpenVPN على هاتفي؟

نعم. WireGuard متعدد المنصات، وله تطبيقات لأنظمة Windows وmacOS وLinux وiOS وAndroid، وتتوفر عملاء OpenVPN للأنظمة نفسها. وتتيح معظم تطبيقات VPN اختيار أحدهما. [1]

Q10: لماذا WireGuard صغير الحجم إلى هذا الحد؟

يدعم WireGuard مجموعة ثابتة واحدة من الشيفرات الحديثة بدلًا من خيارات عديدة. ويحتاج تنفيذه على Linux إلى أقل من 4,000 سطر من الشيفرة، مما يسهّل تدقيقه مقارنة بقواعد شيفرة VPN الأكبر. [3]

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.

Q2: ما الأصفار (الشيفرات) التي يستخدمها WireGuard؟

يستخدم WireGuard شيفرة ChaCha20 مع Poly1305 للتشفير، وCurve25519 لتبادل المفاتيح، وBLAKE2s للتجزئة، وإطار Noise للمصافحة. ولا يوجد تفاوض على الشيفرات، لذا لا يستطيع المستخدمون اختيار خيار ضعيف. [2]

Q3: ما الأصفار (الشيفرات) والمكتبات التي يمكن لـ OpenVPN استخدامها؟

يتكامل OpenVPN بإحكام مع مكتبة OpenSSL ويستخدم TLS لتبادل المفاتيح. ويمكن للمسؤولين اختيار شيفرات قناة البيانات مثل AES-256-GCM، ما يضيف مرونة لكنه يتيح أيضًا مجالًا لإعدادات ضعيفة. [4]

Q4: كيف يصادق كل بروتوكول على الأطراف النظيرة؟

يتعرف أقران WireGuard على بعضهم بمفاتيح عامة ثابتة، على غرار تبادل مفاتيح SSH، ويرتبط كل مفتاح بعناوين IP المسموح بها للنفق. أما OpenVPN فيعتمد عادةً على سلطة شهادات مع شهادات X.509، وغالبًا مع اسم مستخدم وكلمة مرور.

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: ماذا يحدث عند التبديل من Wi-Fi إلى بيانات الهاتف المحمول؟

WireGuard بلا اتصال دائم: يرسل الحزم من العنوان الجديد ويستمر النفق بعد مصافحة سريعة. أما OpenVPN فيحتفظ بحالة الجلسة، لذا قد يتطلب تغيير الشبكة إعادة اتصال تستغرق وقتًا أطول قليلًا.

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: هل لا يزال OpenVPN خيارًا جيدًا إذا كان WireGuard أسرع؟

نعم. OpenVPN ناضج وواسع الانتشار، ويعمل عبر TCP عند حظر UDP، ويدعم الإعدادات المؤسسية المعتمدة على الشهادات. ويقدم كثير من المزوّدين كلا البروتوكولين ليتمكن المستخدمون من التبديل إذا كان أحدهما محظورًا أو بطيئًا.

Q9: ما المنافذ التي يستخدمونها؟

المنفذ المعياري لـ OpenVPN هو 1194، لكن يمكن نقله إلى أي منفذ UDP أو TCP، بما فيها 443. ويستمع WireGuard إلى منفذ UDP يُحدَّد في تهيئته؛ و51820 هو المنفذ المستخدم في أمثلته الرسمية.

Q10: أي بروتوكول أسهل في الإعداد يدويًا؟

WireGuard عادةً أبسط: تُنشئ زوج مفاتيح، وتتبادل المفاتيح العامة، وتسرد عناوين IP المسموح بها. أما OpenVPN فيحتاج إلى شهادات وسلطة شهادات وخيارات أكثر، رغم أن ملفات .ovpn تجمعها في ملف واحد.

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. وسيلتا نقل

يمكن لـ OpenVPN نقل نفقه عبر UDP أو TCP، وفي وضع TLS تشترك قناتا التحكم والبيانات فيه في منفذ واحد. [4]

3. ثورة WireGuard

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

4. التشفير الحديث

يجمع WireGuard بين ChaCha20 وPoly1305 وCurve25519 وBLAKE2s وSipHash24 وHKDF داخل إطار بروتوكول Noise، دون خيارات تشفير قد يخطئ المستخدمون في اختيارها. [2]

5. OpenSSL داخل OpenVPN

يتكامل OpenVPN بإحكام مع مكتبة OpenSSL ويستمد منها كثيرًا من قدراته التشفيرية، بما فيها TLS المستخدم لتبادل المفاتيح. [4]

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. مفاتيح على نمط SSH

تُنشأ اتصالات WireGuard بتبادل مفاتيح عامة بسيطة، على غرار تبادل مفاتيح SSH، دون الحاجة إلى سلطة شهادات. [1]

8. متعدد المنصات

صدر WireGuard أولًا لنواة Linux وهو متاح الآن لأنظمة Windows وmacOS وBSD وiOS وAndroid، لذا يعمل البروتوكول نفسه على معظم الأجهزة. [1]

9. السرية المستقبلية

يكرر WireGuard مصافحة Noise_IK كل بضع دقائق لتدوير مفاتيح الجلسة المتماثلة، مما يوفر سرية أمامية مثالية حتى لو تسرب مفتاح طويل الأمد لاحقًا. [2]

10. واجهات TUN/TAP

صُمم OpenVPN للعمل مع واجهة الشبكة الافتراضية TUN/TAP المتوفرة على معظم المنصات والتي تنقل حزم النفق. [4]

المراجع والمصادر التقنية

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

المراجع الأكاديمية والصناعية

[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] WireGuard. (n.d.). Quick Start.
https://www.wireguard.com/quickstart/

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

مفتاح الإجابة: مقارنة بروتوكولي WireGuard وOpenVPN وأحجام الشيفرة والسرعة، ومعايير التشفير

1 **حجم شيفرة WireGuard** البروتوكولات — **الإجابة الصحيحة: D**

ملاحظة للمعلم

WireGuard مدمج للغاية، ويعمل بنحو 4,000 سطر من الشيفرة. وهذا يُبقي سطح الهجوم صغيرًا ويسهّل التدقيق. الاستشهاد: WireGuard Project.

2 **سرعة فضاء النواة** زمن الاستجابة — **الإجابة الصحيحة: B**

ملاحظة للمعلم

بالتنفيذ مباشرةً في فضاء النواة، يتجنب WireGuard حمل تبديل السياق، مما يتيح معدل نقل مرتفعًا. الاستشهاد: WireGuard Project.

3 **السؤال 3** — **الإجابة الصحيحة: B**

ملاحظة للمعلم

يرتبط OpenVPN ارتباطًا وثيقًا بـ OpenSSL، الذي يوفر شيفرات مثل AES-GCM ويجعله قابلًا للتهيئة بدرجة كبيرة لكنه أكثر تعقيدًا.

4 **أداء البروتوكول** ضوابط التوجيه — **الإجابة الصحيحة: A**

ملاحظة للمعلم

يُنشئ WireGuard المصافحات في أجزاء من الثانية ويستجيب فورًا للتنقل بين الشبكات (مثل التبديل من Wi-Fi إلى الشبكة الخلوية). الاستشهاد: Microsoft Native Gateway, Apple Support. [3]

5 **التشفير غير المتماثل** الخصوصية — **الإجابة الصحيحة: C**

ملاحظة للمعلم

يستخدم WireGuard التوجيه المبني على المفاتيح التشفيرية Cryptokey Routing، الذي يربط المفاتيح العامة بعناوين IP المسموح بها للنفق، على غرار إعدادات SSH. الاستشهاد: WireGuard Project.

مفتاح الإجابة: نقطة التحقق 2 - صحيح أو خطأ

6 **السؤال 6**

الإجابة الصحيحة: صحيح

ملاحظة للمعلم

يبلغ تنفيذ WireGuard على Linux أقل من 4,000 سطر، لذا تستطيع الفرق الأمنية مراجعته أسرع بكثير من قواعد شيفرة VPN الأكبر مثل OpenVPN.

7 **زمن استجابة فضاء المستخدم** السرعات

الإجابة الصحيحة: خطأ

ملاحظة للمعلم

يعمل OpenVPN في فضاء المستخدم، فيمرر الحزم ذهابًا وإيابًا من واجهة النواة الافتراضية، ما يضيف عبء تبديل السياق (ما لم يُستخدم تفريغ النواة مثل OpenVPN DCO). المرجع: DD-WRT custom firmware.

8 **تهيئة OpenVPN** خطر التنصت

الإجابة الصحيحة: صحيح

ملاحظة للمعلم

يدعم OpenVPN العمل عبر TCP (للموثوقية/تجاوز جدران الحماية) أو UDP (للسرعة)، ما يجعله متوافقًا مع جدران حماية المؤسسات المعقدة. المرجع: IETF Cryptographic Protocols.

9 **التشفير الحديث** جدران الحماية

الإجابة الصحيحة: صحيح

ملاحظة للمعلم

يستغني WireGuard عن الشيفرات القديمة لصالح أساسيات حديثة وآمنة مثل ChaCha20 وPoly1305، وتعمل بسرعة على معالجات الجوال. الاستشهاد: WireGuard Project.

10 **تبسيط أزواج المفاتيح** بلا سجلات

الإجابة الصحيحة: خطأ

ملاحظة للمعلم

لا يستخدم WireGuard الشهادات ولا تسلسلات سلطات الشهادات المعقدة؛ بل يعتمد على أزواج بسيطة من المفاتيح العامة/الخاصة تتبادلها الأطراف. الاستشهاد: WireGuard Project.

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

G 1. WireGuard	H 2. OpenVPN	E 3. فضاء النواة	A 4. فضاء المستخدم
B 5. 4,000 سطر	C 6. OpenSSL	F 7. زوج المفاتيح	D 8. TCP/UDP

نقطة التحقق 3: مفتاح الإجابة – المصطلحات الأساسية

1 وايرغارد	2 OpenVPN	3 النواة	4 المستخدم
5 المفاتيح	6 التدقيق		

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

1 F – المكتبة	2 C – النواة	3 B – اوبن	4 G – المفاتيح
5 H – النقل	6 E – التدقيق	7 A – وايرغارد	8 D – المستخدم

ملاحظات النقاش للمعلمين

المصطلحات الأساسية:
تحقّق من قدرة الطلاب على شرح WireGuard وOpenVPN وفضاء النواة 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

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

حل الكلمات المتقاطعة

		د	ر	ا	غ	ر	ي	ا	و	
				ل				ل		
ح	ي	ت	ا	ف	م	ل	ا	ن	ب	و	ا
			ل		س		ل	و		
			م		ت		ت	ا		
			ك		خ		د	ة		
			ت		د		ق			
			ب		م		ي			
			ة			ل	ق	ن	ل	ا

دليل المعلم لحلول الكلمات المتقاطعة

أفقي

1 أفقي: وايرغارد بروتوكول VPN حديث مصمم للسرعة العالية وسهولة تدقيق الشفرة (8 حروف)

4 أفقي: اوبن بروتوكول قديم متين بقاعدة شفرة كبيرة وإعدادات معقدة (4 حروف)

5 أفقي: المفاتيح رموز غير متماثلة يستخدمها WireGuard للتحقق من اتصالات الأقران (8 حروف)

7 أفقي: النقل بروتوكولات نقل يدعمها OpenVPN؛ أما WireGuard فيعمل فوق UDP فقط (5 حروف)

عمودي

2 عمودي: النواة منطقة تنفيذ نظام التشغيل التي يعمل فيها WireGuard طلبا للسرعة (6 حروف)

3 عمودي: المستخدم منطقة التنفيذ التي يعمل فيها OpenVPN مما يخلق عبء تبديل السياق (8 حروف)

5 عمودي: التدقيق حجم قاعدة شفرة WireGuard المدمج الذي يجعل مراجعتها أسهل بكثير (7 حروف)

6 عمودي: المكتبة مكتبة تشفير يعتمد عليها OpenVPN لخوارزميات الشفرات (7 حروف)

مفتاح حل الكلمات المبعثرة والشيفرة

مفتاح تصحيح لنشاط فك خلط مفردات المصطلحات وتحدي الشيفرة السرية.

مفتاح ترتيب الكلمات المبعثرة

1. ررغوادي — وايرغارد
2. ةاناول — النواة
3. داققتيل — التدقيق
4. فيحتاالم — المفاتيح
5. نابو — اوبن
6. دمسخاتلم — المستخدم
7. ابتةلكم — المكتبة
8. لانقل — النقل

مفتاح تحدي الشيفرة السرية

"طور اتصالك القديم بنفق أسرع"

مفتاح إجابات دراسات الحالة

A السيناريو A: اختيار بروتوكول

التنصت والتشفير
معضلة سارة

دليل التصحيح

ينبغي أن تغطي إجابات الطلاب النقاط التالية:

- التوصية: WireGuard. فتصميمه الخفيف عديم الاتصال (connectionless) يتيح للنفق التعافي بسرعة عند تغيّر شبكتها، كما يحافظ ChaCha20-Poly1305 على سرعة التشفير.
- الأمان: يشفّر كلا البروتوكولين حركة مرورها على شبكة Wi-Fi في المقهى، لذا فإن أيًّا منهما يحمي بيانات تسجيل دخولها عند إعداده بشكل صحيح؛ ويؤثر الاختيار أساسًا في السرعة والاستقرار.

B السيناريو B: تجاوز حظر VPN

الحجب الجغرافي وعناوين IP
معضلة Alex

دليل التصحيح

ينبغي أن تغطي إجابات الطلاب النقاط التالية:

- سبب الحجب: يستخدم WireGuard بروتوكول UDP فقط، ومن المرجح أن جدار حماية الفندق يحجب UDP أو يتعرف على حزم WireGuard عبر التصفية أو الفحص العميق للحزم.
- كيف يساعد OpenVPN: يمكنه العمل عبر TCP، بما في ذلك المنفذ 443 الذي يستخدمه HTTPS، والذي نادرًا ما تحجبه جدران حماية الفنادق تمامًا لأن تصفح الويب يعتمد عليه.