الاسم: _____ التاريخ: _____ الدرجة: _____

VPN للوصول عن بُعد

تأمين نقاط نهاية القوى العاملة عن بُعد، والمصادقة متعددة العوامل، وإعدادات أنفاق IPsec.

نظرة تعليمية عامة على شبكات VPN للوصول عن بُعد

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 شبكات VPN للوصول عن بُعد. ستستكشف أنفاق العميل إلى الموقع، وتسجيلات الدخول متعددة العوامل، وفحوصات الوضع الأمني لنقاط النهاية، وحدود النطاق الترددي، وتدقيق أمان syslog.

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/best-vpn-for-business/remote-access/

خارطة طريقك لتعلّم VPN للوصول عن بُعد

- نقاط نهاية آمنة للقوى العاملة عن بُعد تصل إلى عقد الشبكة المحلية.
- هيّئ سياسات المصادقة متعددة العوامل لعمليات تسجيل الدخول عن بُعد.
- إعداد تكوينات IPsec وOpenVPN من العميل إلى الموقع.
- دقّق في سجلات الاتصال عن بُعد بحثًا عن انتهاكات التحكم في الوصول.
- طبّق فحوصات حالة الجهاز قبل منح الاتصال بالشبكة.
- حسّن معدل نقل الخادم لمنع اختناق عرض النطاق للعمل عن بُعد.

تعليمات شبكات VPN للوصول عن بُعد

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 فحوصات الوضع الأمني وتسجيلات الدخول متعددة العوامل. واختم بالنشاط الإضافي «فكّر بسرعة».

أنفاق من العميل إلى الموقع والامتثال لنقاط النهاية (مقدمة)

تنشئ شبكات VPN للوصول عن بُعد أنفاقًا آمنة بين العميل والموقع للموظفين خارج المقر. ويتطلب تأمين هذه الاتصالات فرض تسجيل الدخول بالمصادقة متعددة العوامل (MFA)، وإجراء فحوصات امتثال وضع نقطة النهاية، وتدقيق السجلات عبر مجمّعات syslog المركزية.

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

نقطة التحقق 1: تحدي الاختيار من متعدد

1. ما معيار المصادقة الذي ينبغي أن تفرضه بوابات الوصول عن بُعد عبر VPN؟
   - A) متعدد العوامل
   - B) عامل واحد
   - C) غير مشفّر
   - D) ضيف محلي

2. ما البروتوكول القياسي لتأمين اتصالات العميل بالموقع للعمل عن بُعد؟
   - A) OpenVPN
   - B) SOCKS5
   - C) PPTP
   - D) FTP

3. ما الفحص الذي يتحقق من سلامة حاسوب محمول بعيد قبل الاتصال؟
   - A) فحص الوضع الأمني
   - B) اختبار السرعة
   - C) اختبار Ping
   - D) عدد الذاكرة

4. أين تُخزَّن سجلات اتصال العاملين عن بُعد لأغراض التدقيق الأمني؟
   - A) خادم Syslog
   - B) مفتاح السجل
   - C) ذاكرة العميل
   - D) متصفح الويب

5. ما المشكلة التي تحدث عندما يتجاوز عدد العاملين عن بُعد سعة النطاق الترددي للبوابة؟
   - A) اختناق النطاق الترددي
   - B) تسريب DNS
   - C) اجتياز المصافحة
   - D) انكشاف IP

نقطة التحقق 2: تحدي صحيح أم خطأ

6 سؤال 6

6. تضيف المصادقة متعددة العوامل رمز تحقق ثانويًا لتأمين عمليات تسجيل الدخول عن بُعد.

صحيح ○ خطأ ○

7 سؤال 7

7. تسمح فحوص الوضع الأمني للأجهزة البعيدة ذات جدران الحماية المعطلة بالوصول إلى الخوادم الخاصة.

صحيح ○ خطأ ○

8 سؤال 8

8. سجلات VPN للوصول عن بُعد ضرورية لتتبع الدخول غير المصرح به إلى شبكة الشركة.

صحيح ○ خطأ ○

9 سؤال 9

9. OpenVPN وIPsec بروتوكولان قديمان يفشلان في تشفير بيانات العملاء البعيدين.

صحيح ○ خطأ ○

10 سؤال 10

10. يحدث اختناق عرض النطاق الترددي في البوابة عندما تتجاوز حركة البيانات عن بُعد سعة بطاقة الاتصال.

صحيح ○ خطأ ○

نقطة التحقق 3: إدراج المصطلحات الأساسية

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

1. لحماية بوابات الشركة، يجب أن تتطلب عمليات الدخول عن بعد مصادقة _____ .
2. يشفر العملاء عن بعد حمولات النفق باستخدام بروتوكولات _____ القياسية.
3. يجب أن تجتاز الأجهزة فحصاً أمنياً لـ _____ قبل الحصول على روابط الشبكة.
4. تُرسل سجلات الدخول القابلة للتدقيق باستمرار إلى خادم _____ مركزي.
5. قد تؤدي الحركة الكثيفة في ساعات العمل إلى ازدحام في _____ البوابة.
6. تتولى برامج تشغيل المحول الافتراضي إدارة _____ من العميل إلى الموقع في Windows وmacOS.

بنك كلمات المفردات

الأنفاق السجلات بروتوكول عرض النطاق متعددة العوامل وضع الجهاز OpenVPN Syslog

اكتب إجاباتك هنا:

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

نقطة التحقق 4: مطابقة المفاهيم الأساسية

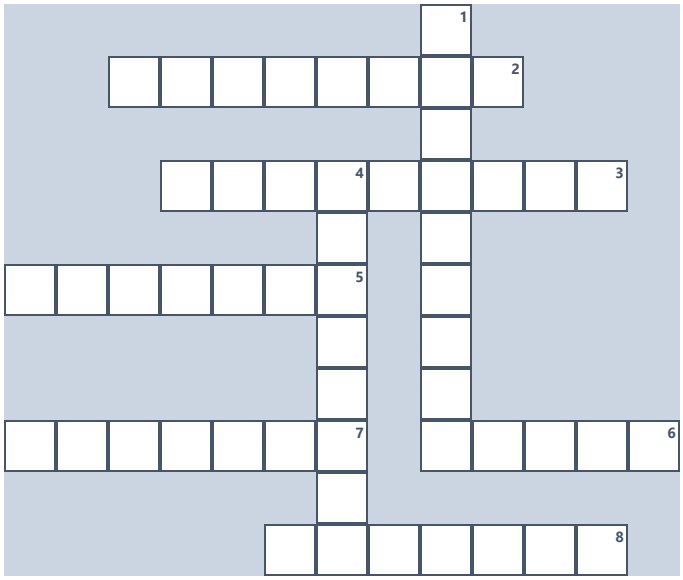
مطابقة التعريفات

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

1. متعدد العوامل	A	تغليف البيانات في مسار آمن.
2. OPENVPN	B	مجمّع مركزي لسجلات الأمان.
3. الوضع الأمني	C	حد سعة بيانات الشبكة.
4. SYSLOG	D	بروتوكول قياسي من العميل إلى الموقع.
5. عرض النطاق الترددي	E	التحقق من سلامة الجهاز البعيد.
6. التشفير	F	قواعد نظام تصفية حركة المرور.
7. الأنفاق (Tunneling)	G	تعمية تشفيرية للحزم.
8. جدار الحماية	H	أمان تسجيل الدخول الذي يتطلب رموزًا إضافية.

نقطة التحقق 5: لغز الكلمات المتقاطعة

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



أفقي

2. معيار قياسي للاتصال من العميل إلى الموقع (8)

3. التحقق من سلامة الجهاز عن بعد (9)

5. أمان تسجيل الدخول بطلب رموز إضافية (7)

6. تغليف البيانات في مسار آمن (5)

7. مجمّع مركزي لسجلات الأمان (7)

8. تشويش الحزم بطريقة تشفيرية (7)

عمودي

1. حد سعة بيانات الشبكة (9)

4. قواعد نظام تصفية الحركة (8)

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: معيار قياسي للاتصال من العميل إلى الموقع (8 حروف):

3 أفقي: التحقق من سلامة الجهاز عن بعد (9 حروف):

5 أفقي: أمان تسجيل الدخول بطلب رموز إضافية (7 حروف):

6 أفقي: تغليف البيانات في مسار آمن (5 حروف):

7 أفقي: مجمّع مركزي لسجلات الأمان (7 حروف):

8 أفقي: تشويش الحزم بطريقة تشفيرية (7 حروف):

عمودي

1 عمودي: حد سعة بيانات الشبكة (9 حروف):

4 عمودي: قواعد نظام تصفية الحركة (8 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.

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

قائمة كلمات المفردات

العوامل
بروتوكول
وضعالجهاز
السجلات
عرضالنطاق
التشفير
النفق
جدارناري

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. العوامل
B. بروتوكول
C. وضعالجهاز
D. السجلات
E. عرضالنطاق
F. التشفير
G. النفق
H. جدارناري

التعريفات وحقول المطابقة
1. مجمّع مركزي لسجلات الأمان.
2. قواعد نظام تصفية الحركة.
3. تغليف البيانات في مسار آمن.
4. تشويش الحزم بطريقة تشفيرية.
5. معيار قياسي للاتصال من العميل إلى الموقع.
6. حد سعة بيانات الشبكة.
7. التحقق من سلامة الجهاز عن بعد.
8. أمان تسجيل الدخول بطلب رموز إضافية.

نقطة التحقق 7: تحدي الكلمات المبعثرة

أعد ترتيب الحروف أدناه للكشف عن المفاهيم الأساسية في ورقة العمل هذه. اكتب إجاباتك في مربعات الإدخال المخصصة.

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

نشاط إضافي: فكّر بسرعة

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

1	خرافات عن VPN			
2	كلمات تصف الثقة المعدومة (Zero Trust)			
3	برامج مكتبية تعرفها			
4	قواعد للعمل عن بُعد بأمان			
5	أشياء يستطيع مزوّد الإنترنت رؤيتها			
6	خدمات VPN التي تعرفها			
7	أماكن يعمل منها الموظفون			
8	أدوات تستخدمها الشركة كل يوم			
9	أدوار في قسم تقنية المعلومات			
10	أجهزة قد يملكها الموظف			
11	بيانات يجب على الشركة حمايتها			
12	أشياء تفعلها بعد خرق أمني			
13	أشياء قد تعطّل اجتماع الفيديو			
14	طرق لتسجيل الدخول بأمان			
15	أسباب لتزويد الموظفين بـ VPN			

نقطة التحقق 8: دراسات حالة في VPN والشبكات

طبّق المفاهيم التي تعلمتها لحل السيناريوهات الواقعية أدناه.

دراسة الحالة 1: فرض المصادقة متعددة العوامل



السيناريو: يحاول محلل أعمال تسجيل الدخول إلى قاعدة بيانات شركته أثناء العمل عن بُعد. يدخل اسم المستخدم وكلمة المرور الصحيحين، لكن بوابة VPN تمنع الوصول وتطلب رمز من مفتاح مادي.

سؤال للنقاش: أي سياسة أمنية تفرض خطوة التحقق المزدوج هذه؟

دراسة الحالة 2: الامتثال للوضع الأمني



السيناريو: يوصل متعاقد حاسوبه المحمول الشخصي بشبكة الشركة عن بُعد. يقطع عميل VPN الاتصال فورًا، ويُعلم المستخدم بأن تعريفات مكافحة الفيروسات لديه قديمة.

سؤال للنقاش: ما فحص بوابة VPN المتخصص الذي منع محاولة الاتصال هذه؟

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

8	28	18	2	23	1		23	27	14	27	23	1		28	24	6	28
29	18	11	27	24	23	1		29	12	12	32	24	23	1		16	1	21	25

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 VPN للوصول عن بُعد؟

طريقة اتصال آمنة تمكّن الموظفين العاملين خارج المقر من الاتصال مباشرة بخوادم الشركة الخاصة.

Q2: ما الفرق بين اتصال العميل بالموقع واتصال الموقع بالموقع؟

يربط نمط العميل إلى الموقع أجهزة المستخدمين الفردية، بينما يربط نمط الموقع إلى الموقع مواقع مكاتب فعلية كاملة.

Q3: ما فحص وضعية الجهاز؟

فحص يتحقق من الحالة الأمنية لجهاز بعيد (مكافحة الفيروسات، مستوى تحديث النظام) قبل منح الوصول.

Q4: لماذا يُستخدم OpenVPN للوصول عن بُعد؟

بسبب بروتوكوله الأمني القوي وتوافقه مع منصات متعددة وقدرته على التعامل مع الاتصالات الفردية.

Q5: كيف تحمي المصادقة متعددة العوامل (MFA) الوصول عن بُعد؟

يضيف رمز تحقق ثانويًا، فيمنع الوصول حتى لو سُرّبت كلمات مرور الموظفين أو سُرقت.

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

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

Q6: ما خادم syslog؟

مستودع سجلات مركزي يخزّن أحداث الاتصال وتسجيلات الدخول وتنبيهات النظام لعمليات التدقيق في الامتثال.

Q7: ما أسباب اختناق عرض النطاق؟

عندما تتجاوز متطلبات النطاق الترددي المجمّعة للموظفين عن بُعد الحد الأقصى لسرعة إنترنت بوابة الشركة.

Q8: هل يمكنني ربط حاسوبي المنزلي بشبكة VPN الخاصة بالعمل؟

فقط إذا اجتاز الجهاز عمليات تدقيق فحص الوضع الأمني للشركة وأذن به مسؤولو تقنية المعلومات.

Q9: ما تغليف الشبكة (network encapsulation)؟

تغليف حزم البيانات أثناء النقل داخل ترويسات بروتوكول مشفرة لتأمين الإرسال.

Q10: كيف يحسّن النفق المقسَّم الوصول عن بُعد؟

يتيح للموظفين استخدام مزوّد خدمة الإنترنت المحلي للتصفح العادي مع توجيه الملفات المتعلقة بالعمل عبر VPN.

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

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

Q1: كيف تعزز المصادقة المعتمدة على الشهادات الوصول عن بُعد؟

يربط أذونات الاتصال بشهادات رقمية محلية مثبتة مسبقًا، فيحجب الأجهزة غير المُدارة أو غير المصرح بها.

Q2: ما الخطر الأمني للنفق المقسَّم في العمل عن بُعد؟

يخلق جسرًا محتملًا يمكن من خلاله لجهاز محلي مخترق توجيه التهديدات الخارجية إلى الشبكة الخاصة.

Q3: كيف تفحص عمليات التحقق من الوضعية إعدادات السجل (registry)؟

يشغّل عميل VPN نصوصًا برمجية محلية تستعلم عن مسارات السجل (registry) للتحقق مما إذا كانت برمجيات الأمان في الشركة تعمل بنشاط.

Q4: لماذا تستخدم سجلات النظام (syslogs) المنفذ UDP 514 افتراضيًا؟

لنقل السجلات بسرعة وبأقل حمل ممكن، رغم أن الإعدادات الآمنة تشترط الآن تغليف TLS عبر TCP.

Q5: كيف تحل الشركات اختناقات عرض النطاق الترددي في البوابة؟

بتنفيذ موازنات الأحمال وتوزيع الحركة البعيدة على عقد الخوادم الإقليمية.

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

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

Q6: ما وظيفة محولات TAP/TUN الافتراضية على العملاء البعيدين؟

تعمل كبطاقات شبكة افتراضية، وتوجّه حركة TCP/IP على مستوى الجهاز مباشرة إلى نفق VPN المشفر.

Q7: كيف يدعم IKEv2 MOBIKE تنقل القوى العاملة عن بُعد؟

يحدّث ديناميكيًا ارتباطات عناوين IP، فيُبقي VPN نشطًا أثناء تنقل المستخدم بين Wi-Fi وبيانات الجوال.

Q8: ما الفرق بين التوجيه المجزّأ والتوجيه عبر النفق الكامل؟

يفرض التوجيه الكامل مرور جميع حركة الإنترنت من الجهاز عبر VPN، بينما يرسل التوجيه المقسّم عناوين IP الخاصة بوجهات الشركة فقط.

Q9: كيف تتعامل أجهزة NAT مع اتصالات VPN البعيدة؟

بربط نطاقات المنافذ المحلية بعناوين IP لبوابة عامة لتوجيه حزم البيانات المشفّرة العائدة.

Q10: ما معايير الامتثال التي تفرض تدقيق الوصول عن بُعد؟

تتطلب معايير مثل HIPAA وSOC 2 وPCI DSS تسجيل جميع جلسات الاتصال البعيد ومراقبتها.

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

تنشئ شبكات VPN للوصول عن بُعد أنفاقًا آمنة بين العميل والموقع للعاملين خارج المقر.

2. نظرة على VPN

تشترط قواعد الامتثال المصادقة متعددة العوامل لحماية بوابات الأعمال عن بُعد.

3. نظرة على VPN

تتحقق فحوص الوضع الأمني من إعدادات أمان العميل المحلي قبل منح الوصول إلى الشبكة الخاصة.

4. نظرة على VPN

تجمع خوادم Syslog سجلات الاتصال لتدقيق محاولات الوصول غير المصرح بها واكتشافها.

5. نظرة على VPN

يحدث اختناق عرض النطاق الترددي في البوابة عندما تتجاوز متطلبات حركة البيانات عن بُعد المجمّعة حدود إنترنت الخادم.

6. نظرة على VPN

تغلّف مهايئات الشبكة الافتراضية استعلامات شبكة نظام التشغيل داخل بروتوكولات آمنة.

7. رؤية حول VPN

يتيح دعم MOBIKE للعملاء البعيدين التبديل بين الشبكات دون قطع نفق VPN.

8. رؤية حول VPN

يؤمّن توجيه النفق الكامل جميع حركة الإنترنت للعاملين لكنه يزيد الحمل على بوابة الشركة.

9. رؤية حول VPN

تربط مصادقة الشهادات تفويض اتصال VPN مباشرةً بالعتاد الذي تديره الشركة.

10. نظرة على VPN

تتوقع أطر مثل SOC 2 وPCI DSS تسجيل جلسات الوصول عن بُعد ومراقبتها.

المراجع والمصادر التقنية

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

المراجع الأكاديمية والصناعية

[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/

[5] IETF. (2006). RFC 4555: IKEv2 Mobility and Multihoming Protocol (MOBIKE).
https://www.rfc-editor.org/rfc/rfc4555

مفتاح الإجابة: نقطة التحقق 1 - اختيار من متعدد

1 رموز تسجيل الدخول — أمان MFA — الإجابة الصحيحة: A

ملاحظة للمعلم

تفرض المصادقة متعددة العوامل تحققًا ثانويًا عند تسجيل الدخول. المصدر: MFA Implementation.

2 نفق OpenVPN — من العميل إلى الموقع — الإجابة الصحيحة: A

ملاحظة للمعلم

OpenVPN بروتوكول معياري لتأمين أنفاق العميل إلى الموقع. المرجع: OpenVPN Client.

3 تدقيقات الوضع الأمني — فحص الجهاز — الإجابة الصحيحة: A

ملاحظة للمعلم

تفحص فحوص الوضع الأمني نقاط النهاية بحثًا عن جدران حماية وأدوات مكافحة فيروسات نشطة. المرجع: Posture Compliance.

4 مجمّع السجلات — خادم SYSLOG — الإجابة الصحيحة: A

ملاحظة للمعلم

تجمع خوادم Syslog سجلات الأحداث الأمنية لمراقبة انتهاكات الوصول. المصدر: Syslog Standard.

5 Card Overflow — اختناق البوابة — الإجابة الصحيحة: A

ملاحظة للمعلم

يحدث اختناق عرض النطاق الترددي في البوابة عندما تتجاوز حركة بيانات المستخدمين حدود الخادم. المصدر: Capacity Planning.

مفتاح الإجابة: نقطة التحقق 2 - صحيح أو خطأ

6 رموز تسجيل الدخول — فحوصات MFA — الإجابة الصحيحة: صحيح

ملاحظة للمعلم

تفرض المصادقة متعددة العوامل تحققًا ثانويًا عند تسجيل الدخول. المصدر: MFA Implementation.

7 السؤال 7 — الإجابة الصحيحة: خطأ

ملاحظة للمعلم

تحظر فحوصات الوضع الأمني الأجهزة التي يكون جدار الحماية أو برنامج مكافحة الفيروسات فيها متوقفًا، لذا تُمنع هذه الأجهزة.

8 مجمّع السجلات — خادم SYSLOG — الإجابة الصحيحة: صحيح

ملاحظة للمعلم

تجمع خوادم Syslog سجلات الأحداث الأمنية لمراقبة انتهاكات الوصول. المصدر: Syslog Standard.

9 السؤال 9 — الإجابة الصحيحة: خطأ

ملاحظة للمعلم

OpenVPN وIPsec بروتوكولان حاليان يشفّران حركة العملاء عن بُعد فعلًا.

10 Card Overflow — اختناق البوابة — الإجابة الصحيحة: صحيح

ملاحظة للمعلم

يحدث اختناق عرض النطاق الترددي في البوابة عندما تتجاوز حركة بيانات المستخدمين حدود الخادم. المصدر: Capacity Planning.

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. متعدد العوامل	D 2. OPENVPN	E 3. الوضع الأمني	B 4. SYSLOG
C 5. عرض النطاق الترددي	G 6. التشفير	A 7. الأنفاق (Tunneling)	F 8. جدار الحماية

نقطة التحقق 3: مفتاح الإجابة – المصطلحات الأساسية

1 متعددة العوامل	2 OpenVPN	3 وضع الجهاز	4 Syslog
5 عرض النطاق	6 الأنفاق		

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

1 D – السجلات	2 H – جدارناري	3 G – النفق	4 F – التشفير
5 B – بروتوكول	6 E – عرضالنطاق	7 C – وضعالجهاز	8 A – العوامل

ملاحظات النقاش للمعلمين

المصطلحات الأساسية:
تحقّق من قدرة الطلاب على شرح متعدد العوامل وOPENVPN والوضع الأمني بكلماتهم الخاصة وإعطاء مثال على كل منها.

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

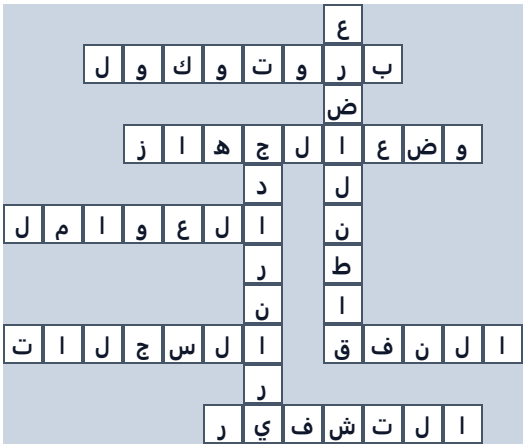
تقييم المصادر:
اطلب من الطلاب التحقق من ادعاء واحد على الأقل من مراجع ورقة العمل، وناقش لماذا قد تتغير الأرقام والأسعار والقواعد مع الوقت.

مفاتيح الألغاز وملاحظات المعلم

حل البحث عن الكلمات

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

حل الكلمات المتقاطعة



دليل المعلم لحلول الكلمات المتقاطعة

أفقي

2 أفقي: بروتوكول معيار قياسي للاتصال من العميل إلى الموقع (8 حروف)

3 أفقي: وضعالجهاز التحقق من سلامة الجهاز عن بعد (9 حروف)

5 أفقي: العوامل أمان تسجيل الدخول بطلب رموز إضافية (7 حروف)

6 أفقي: النفق تغليف البيانات في مسار آمن (5 حروف)

7 أفقي: السجلات مجمّع مركزي لسجلات الأمان (7 حروف)

8 أفقي: التشفير تشويش الحزم بطريقة تشفيرية (7 حروف)

عمودي

1 عمودي: عرضالنطاق حد سعة بيانات الشبكة (9 حروف)

4 عمودي: جدارناري قواعد نظام تصفية الحركة (8 حروف)

مفتاح حل الكلمات المبعثرة والشيفرة

مفتاح تصحيح لنشاط فك خلط مفردات المصطلحات وتحدي الشيفرة السرية.

مفتاح ترتيب الكلمات المبعثرة

1. ومالعل → العوامل
2. زواضجهلع → وضعالجهاز
3. عنلرطقااض → عرضالنطاق
4. نققال → النفق
5. وكرلتبوو → بروتوكول
6. اسلاجتل → السجلات
7. ايفرلشت → التشفير
8. ردنيجرا → جدارناري

مفتاح تحدي الشيفرة السرية

"يحمي الوصول البعيد نقاط المؤسسة الموزعة"

مفتاح إجابات دراسات الحالة

A دراسة الحالة 1: فرض المصادقة متعددة العوامل

حل المعلم

دليل التصحيح

ينبغي أن تغطي إجابات الطلاب النقاط التالية:

- تحليل السيناريو: يحاول محلل أعمال تسجيل الدخول إلى قاعدة بيانات شركته أثناء العمل عن بُعد. يدخل اسم المستخدم وكلمة المرور الصحيحين، لكن بوابة VPN تحظر الوصول وتطلب رمز مادي.
- الاستراتيجية والحل الموصى بهما: تفرض بوابة VPN المؤسسية سياسة صارمة للمصادقة متعددة العوامل (MFA) لتأمين عمليات تسجيل الدخول عن بُعد.

B دراسة الحالة 2: الامتثال للوضع الأمني

حل المعلم

دليل التصحيح

ينبغي أن تغطي إجابات الطلاب النقاط التالية:

- تحليل السيناريو: يوصل مقاول حاسوبه المحمول الشخصي بشبكة الشركة عن بُعد. يقطع عميل VPN الاتصال فورًا ويبلغ المستخدم بأن تعريفات مكافحة الفيروسات لديه قديمة.
- الاستراتيجية والحل الموصى بهما: أجرت بوابة الوصول عن بُعد فحص وضع نقطة النهاية وحظرت الجهاز بسبب إعدادات أمنية قديمة.