الاسم: _____ التاريخ: _____ الدرجة: _____

VPN للمؤسسات

تنفيذ الوصول إلى الشبكة بنموذج انعدام الثقة، وعقد بوابات مخصصة، وضوابط إدارية مركزية للشركة.

نظرة تعليمية على شبكات VPN للمؤسسات

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 المؤسسية. ستستكشف بنى انعدام الثقة وبوابات IP الثابتة المخصصة ووحدات تحكم المسؤولين والتزويد وأنفاق IPsec من موقع إلى موقع.

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/enterprise/

خارطة طريقك لتعلّم شبكة VPN للمؤسسات

- طبّق أطر الوصول إلى الشبكة بنموذج انعدام الثقة (ZTNA).
- هيّئ عناوين IP لبوابة الخادم المخصص لمرشحات القائمة البيضاء.
- إدارة لوحات الإدارة المؤسسية المركزية وقوائم مقاعد المستخدمين.
- دقّق في سجلات الوصول إلى الشبكة وسجلات اتصال المستخدمين.
- هيّئ قواعد تسجيل الدخول الموحد (SSO) والمصادقة متعددة العوامل.
- إعداد أنفاق IPsec من موقع إلى موقع بين الفروع.

تعليمات شبكات VPN للمؤسسات

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 Zero Trust وIPsec بين المواقع. واختم بالنشاط الإضافي «فكّر بسرعة».

بنى انعدام الثقة والبوابات المخصصة (مقدمة)

تؤمّن شبكات VPN للمؤسسات أصول الشركة بالانتقال إلى أطر الوصول إلى الشبكة بمبدأ انعدام الثقة (ZTNA) ووضع بوابات IP الثابتة المخصصة في قائمة السماح. ويستخدم مديرو تقنية المعلومات لوحات إدارة مركزية لتنسيق أنفاق IPsec من موقع إلى موقع وروابط تسجيل الدخول الموحد (SSO).

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

نقطة التحقق 1: تحدي الاختيار من متعدد

1. ما نموذج الأمان الذي يحل محل شبكات VPN القديمة للمؤسسات؟
   - A) الثقة المعدومة
   - B) قفزات متعددة
   - C) نظير إلى نظير
   - D) بوابة واحدة

2. ما الميزة المطلوبة لقصر الوصول إلى قاعدة البيانات على خوادم الشركة؟
   - A) IP مخصص
   - B) التوجيه الديناميكي
   - C) نفق مقسّم
   - D) وكيل DNS

3. ما البروتوكول القياسي لأنفاق الموقع إلى الموقع في الشركات؟
   - A) IPsec
   - B) PPTP
   - C) SOCKS5
   - D) SSL v3

4. ما الأداة المركزية التي تتيح للمسؤولين إدارة مقاعد الموظفين؟
   - A) وحدة تحكم المسؤول
   - B) مفتاح السجل
   - C) البرامج الثابتة للموجّه
   - D) سجل النظام

5. أي معيار مصادقة يتيح تسجيل الدخول عبر Okta أو Microsoft Entra ID؟
   - A) تسجيل الدخول الموحد (SSO)
   - B) السر المشترك
   - C) مصادقة EPP
   - D) مفتاح WEP

نقطة التحقق 2: تحدي صحيح أم خطأ

6 سؤال 6

6. يمنح الوصول إلى الشبكة بانعدام الثقة الدخول إلى الشبكة فقط بعد التحقق من موثوقية الجهاز بشكل مستمر.

○ صحيح ○ خطأ

7 سؤال 7

7. توجّه بوابات IP المخصصة حركة مرور الموظفين إلى جانب مستخدمين عموميين عشوائيين.

○ صحيح ○ خطأ

8 سؤال 8

8. تتيح وحدات التحكم الإدارية المركزية لمديري تقنية المعلومات إلغاء مقاعد الموظفين الفرديين فورًا.

○ صحيح ○ خطأ

9 سؤال 9

9. IPsec بروتوكول خفيف لا يدعم أنفاق الشبكات بين المواقع.

○ صحيح ○ خطأ

10 سؤال 10

10. يتيح تسجيل الدخول الموحد مصادقة آمنة للموظفين باستخدام مزوّدي هوية الشركة.

○ صحيح ○ خطأ

نقطة التحقق 3: إدراج المصطلحات الأساسية

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

1. تستبدل البنى الأمنية الحديثة الأنفاق القديمة بوصول قائم على _____ .
2. لتقييد الوصول إلى قاعدة البيانات، تضبط الشركات بوابة ذات _____ .
3. تُربط الفروع بأمان باستخدام أنفاق _____ من موقع إلى موقع.
4. يخصص مسؤولو تقنية المعلومات تراخيص المستخدمين للموظفين داخل _____ المركزية.
5. يتيح تكامل Okta للموظفين المصادقة عبر _____ للشركة.
6. لحماية عمليات تسجيل الدخول، تشترط بوابات المؤسسات مصادقة _____ .

بنك كلمات المفردات

الأنفاق البوابة الدخول الموحد انعدام الثقة عنوان IP مخصص متعددة العوامل
وحدة التحكم IPsec

اكتب إجاباتك هنا:

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

نقطة التحقق 4: مطابقة المفاهيم الأساسية

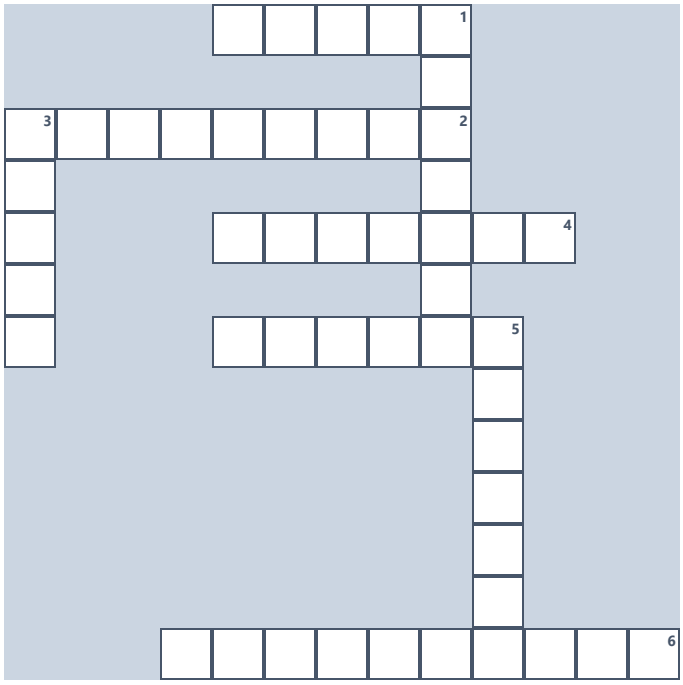
مطابقة التعريفات

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

1. انعدام الثقة	A	تخصيص تراخيص وصول الموظفين إلى VPN.
2. IP مخصص	B	ربط الهوية بين Okta وEntra ID.
3. IPSEC	C	أمان تسجيل الدخول الذي يتطلب رموزًا إضافية.
4. وحدة تحكم المسؤول	D	عنوان بوابة القائمة البيضاء الثابتة.
5. تسجيل الدخول الموحد	E	معيار النفق من موقع إلى موقع.
6. متعدد العوامل	F	عقدة توجيه مدخل الشبكة.
7. البوابة	G	بوابة مقاعد مدير تقنية المعلومات المركزي.
8. التوفير	H	إطار عمل للتحقق المستمر من الثقة.

نقطة التحقق 5: لغز الكلمات المتقاطعة

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



أفقي

1. إطار يتحقق منها باستمرار (5)
2. عنوان بوابة ثابت للقائمة البيضاء (9)
4. معيار الاتصال من موقع إلى موقع (IPsec) (7)
5. ربط الهوية مع Okta و Entra ID (6)
6. بوابة مركزية لمقاعد مدير تقنية المعلومات (10)

عمودي

1. أمان تسجيل الدخول بطلب رموز إضافية (7)
3. منح تراخيص وصول الموظفين إلى VPN (5)
5. عقدة توجيه مدخل الشبكة (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: إطار يتحقق منها باستمرار (5 حروف):

2 أفقي: عنوان بوابة ثابت للقائمة البيضاء (9 حروف):

4 أفقي: معيار الاتصال من موقع إلى موقع (IPsec) (7 حروف):

5 أفقي: ربط الهوية مع Okta وEntra ID (6 حروف):

6 أفقي: بوابة مركزية لمقاعد مدير تقنية المعلومات (10 حروف):

عمودي

1 عمودي: أمان تسجيل الدخول بطلب رموز إضافية (7 حروف):

3 عمودي: منح تراخيص وصول الموظفين إلى VPN (5 حروف):

5 عمودي: عقدة توجيه مدخل الشبكة (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.

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

قائمة كلمات المفردات

الثقة عنوانثابت الانفاق وحدةالتحكم الموحد العوامل البوابة تخصيص

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. الثقة
B. عنوانثابت
C. الانفاق
D. وحدةالتحكم
E. الموحد
F. العوامل
G. البوابة
H. تخصيص

التعريفات وحقول المطابقة
1. عنوان بوابة ثابت للقائمة البيضاء.
2. عقدة توجيه مدخل الشبكة.
3. منح تراخيص وصول الموظفين إلى VPN.
4. أمان تسجيل الدخول بطلب رموز إضافية.
5. معيار الاتصال من موقع إلى موقع (IPsec).
6. إطار يتحقق منها باستمرار.
7. ربط الهوية مع Okta وEntra ID.
8. بوابة مركزية لمقاعد مدير تقنية المعلومات.

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. ق ث ا ة ل
2. ا ا ق ا ف ن ل
3. ا م و د ح ل
4. ة ل ا و ب ا ب
5. ا ن ن ت ث ا ع ب و
6. ك ا ة ت ح و ح ل م د
7. ا م ا ل ل و ع
8. ص ت ص ي خ

نشاط إضافي: فكّر بسرعة

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

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

نقطة التحقق 8: دراسات حالة في VPN والشبكات

طبّق المفاهيم التي تعلمتها لحل السيناريوهات الواقعية أدناه.

دراسة الحالة 1: الانتقال إلى انعدام الثقة



السيناريو: تريد مؤسسة تأمين خوادمها المحلية عن طريق التحقق باستمرار من شهادات امتثال الأجهزة وحالة جدار الحماية وموقع المستخدم بدلًا من الوثوق بأي شخص داخل الشبكة.

سؤال للنقاش: ما الإطار الذي ينبغي على مدير أمن تقنية المعلومات تطبيقه لتحقيق ذلك؟

دراسة الحالة 2: تقييد البوابة



السيناريو: تستضيف شركة قواعد بيانات مالية خاصة في السحابة. تريد حظر كل وصول من الإنترنت العام إلى لوحات الإدارة، والسماح بتسجيل الدخول فقط من نقاط نهاية الشركة الموثّقة.

سؤال للنقاش: ما إعداد الشبكة الذي ينبغي أن يطبقه مسؤول قاعدة البيانات على جدار الحماية السحابي؟

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		21	21	6	3	28		29	21	4	23	1		24	1	8	18	25	1

29	23	14	3	24	23	1		29	11	26	5	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 VPN للمؤسسات؟

نفق شبكي آمن مصمم للشركات، يتيح للعاملين عن بُعد الوصول إلى شبكات الشركة بإدارة مركزية.

Q2: كيف يختلف Zero Trust عن شبكات VPN التقليدية؟

تثق شبكات VPN التقليدية بكل من داخل النفق، بينما يتحقق Zero Trust باستمرار من كل جهاز واتصال مستخدم.

Q3: ما عنوان IP المخصص في شبكات VPN للأعمال؟

عنوان IP ثابت محجوز لشركتك وحدها، يتيح لك إدراجه في القائمة المسموحة للوصول الآمن إلى قواعد البيانات السحابية.

Q4: لماذا يُعد تسجيل الدخول الموحد (SSO) مهمًا لشبكات VPN للأعمال؟

يتيح تسجيل الدخول الموحد (Single Sign-On) للموظفين استخدام بيانات اعتماد الشركة (مثل Okta أو Microsoft Entra ID) لتسجيل الدخول بأمان.

Q5: ما شبكة VPN من موقع إلى موقع؟

نفق يربط مكتبين فعليين (مثل فرع ومقر رئيسي) عبر الإنترنت العام باستخدام IPsec.

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

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

Q6: ما وظيفة وحدة تحكم المسؤول؟

لوحة تحكم لمسؤولي تقنية المعلومات لإضافة مقاعد الموظفين أو إزالتها وتعيين البوابات ومراقبة الاتصالات النشطة.

Q7: كيف تؤمّن المصادقة متعددة العوامل (MFA) شبكات VPN للأعمال؟

باشتراط رمز ثانٍ (مثل رمز تطبيق المصادقة) لمنع الدخول غير المصرّح به من كلمات المرور المخترقة.

Q8: هل يمكنني تدقيق سجل اتصال الموظفين؟

نعم، تسجّل شبكات VPN للمؤسسات أوقات الاتصال ومدته وعناوين IP المُعيَّنة لأغراض التدقيق والامتثال.

Q9: ما ZTNA؟

الوصول إلى الشبكة بانعدام الثقة، وهو نموذج أمني يمنح الوصول إلى تطبيقات محددة فقط بدلًا من الشبكة بأكملها.

Q10: ما دور عقد البوابة؟

تعمل كنقاط دخول آمنة لحركة المرور البعيدة، وتوجّه البيانات مباشرة إلى خوادم الشركة الخاصة.

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

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

Q1: كيف يحمي IPsec الاتصالات المؤسسية بين المواقع؟

يشفّر IPsec حركة البيانات على طبقة الشبكة باستخدام Encapsulating Security Payload (ESP) لضمان سرية البيانات وسلامتها.

Q2: لماذا يفشل الأمن التقليدي القائم على المحيط مع القوى العاملة عن بُعد؟

لأن الموظفين يصلون إلى البيانات من مواقع وأجهزة متعددة، مما يجعل محيط جدار حماية الشبكة الواحد قديمًا.

Q3: كيف ينفّذ مديرو تقنية المعلومات التزويد الآلي؟

بربط بروتوكولات SCIM بين مزودي الهوية (Okta) ووحدة تحكم مسؤول VPN لمزامنة أدلة المستخدمين.

Q4: ما فائدة النفق المجزّأ في بيئات الشركات؟

يوجّه حركة SaaS المحلية (مثل Microsoft 365) خارج نفق VPN، محافظًا على عرض النطاق الترددي لبوابة الشركة لقواعد البيانات الخاصة.

Q5: كيف تتحقق فحوصات وضعية الجهاز من أمان نقاط النهاية؟

يفحص عميل VPN الجهاز قبل الاتصال للتحقق من أن جدار الحماية نشط ومضاد الفيروسات يعمل وتحديثات نظام التشغيل محدّثة.

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

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

Q6: ما دور اجتياز NAT (NAT traversal) في إعدادات VPN للأعمال؟

يغلّف NAT-T حزم IPsec داخل UDP للسماح لها بالمرور عبر موجّهات المنازل وجدران الحماية دون انقطاع الاتصال.

Q7: كيف تمنع الشركات اختناق عرض النطاق في البوابة؟

بنشر عدة عقد بوابات إقليمية وموازنة حركة المستخدمين الواردة بينها باستخدام موازنات الأحمال.

Q8: لماذا تُفضّل القوائم البيضاء لعناوين IP الثابتة على الديناميكية؟

تمنع القوائم البيضاء الثابتة عناوين IP الخارجية غير المصرح بها من محاولة مصافحات الاتصال، مما يقلل سطح الهجوم بشكل كبير.

Q9: ما دور المصادقة القائمة على الشهادات في شبكات VPN المؤسسية؟

يتحقق من الشهادات الرقمية الفريدة المثبتة على الأجهزة التي تديرها الشركة، فيحجب الحواسيب الشخصية غير المُدارة.

Q10: كيف يقلل ZTNA خطر الحركة الجانبية؟

بعزل جلسات المستخدمين عن موارد مصرّح بها محددة، مما يمنع المخترقين من التنقل عبر الشبكة إذا اختُرقت عقدة واحدة.

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

تتحقق بنى انعدام الثقة باستمرار من الحالة الأمنية لكل جهاز يحاول الاتصال بالشبكة.

2. نظرة على VPN

تتيح بوابات IP المخصصة للشركات تأمين قواعد البيانات السحابية عبر وضع العناوين الثابتة في قائمة السماح.

3. نظرة على VPN

IPsec هو البروتوكول القياسي في الصناعة لإعداد أنفاق شبكات المكاتب الآمنة بين المواقع.

4. نظرة على VPN

تتيح وحدات تحكم المسؤول لأقسام تقنية المعلومات توفير مقاعد وصول الموظفين إلى VPN وإدارتها وتدقيقها.

5. نظرة على VPN

يدمج تسجيل الدخول الموحد الوصول إلى VPN مع مزوّدي هوية الشركة مثل Okta وEntra ID.

6. نظرة على VPN

تحجب المصادقة متعددة العوامل محاولات الاتصال غير المصرح بها الناتجة عن مفاتيح كلمات مرور مسروقة.

7. رؤية حول VPN

يحسّن النفق المقسّم النطاق الترددي للشركة باستبعاد حركة SaaS العامة من النفق المشفر.

8. رؤية حول VPN

تتحقق فحوص وضع الجهاز من إعدادات الأمان المحلية قبل منح الوصول إلى خوادم الشركة.

9. رؤية حول VPN

تؤتمت مزامنة دليل SCIM ضوابط وصول الموظفين عند الانضمام والمغادرة.

10. نظرة على VPN

يقصر الوصول إلى الشبكة بانعدام الثقة وصول المستخدم على تطبيقات مصرّح بها محددة، مما يمنع الحركة الجانبية داخل الشبكة.

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/

مفتاح الإجابة: نقطة التحقق 1 - اختيار من متعدد

1 انعدام الثقة — نموذج ZTNA — الإجابة الصحيحة: A

ملاحظة للمعلم

تتحقق نماذج انعدام الثقة من امتثال الجهاز باستمرار قبل الدخول إلى الشبكة. الاستشهاد: NIST Zero Trust.

2 عنوان IP مخصص — IP ثابت — الإجابة الصحيحة: A

ملاحظة للمعلم

تتيح عناوين IP المخصصة وضع البوابات في قائمة السماح لحجب حركة المرور العامة. المصدر: Dedicated IP Guide.

3 معيار IPsec — نفق IPSEC — الإجابة الصحيحة: A

ملاحظة للمعلم

IPsec هو البروتوكول القياسي المستخدم لأنفاق الفروع بين المواقع. المصدر: IPsec Tunneling.

4 تخصيص تقنية المعلومات — وحدة تحكم المسؤول — الإجابة الصحيحة: A

ملاحظة للمعلم

تتيح لوحات المعلومات الإدارية المركزية لمديري تقنية المعلومات تخصيص تراخيص المقاعد. المصدر: إرشادات CISA.

5 السؤال 5 — الإجابة الصحيحة: A

ملاحظة للمعلم

أي معيار مصادقة يتيح تسجيل الدخول عبر Okta أو Microsoft Entra ID؟ ← تسجيل الدخول الموحد (SSO)

مفتاح الإجابة: نقطة التحقق 2 - صحيح أو خطأ

6 انعدام الثقة — فحوصات ZTNA — الإجابة الصحيحة: صحيح

ملاحظة للمعلم

تتحقق نماذج انعدام الثقة من امتثال الجهاز باستمرار قبل الدخول إلى الشبكة. الاستشهاد: NIST Zero Trust.

7 السؤال 7 — الإجابة الصحيحة: خطأ

ملاحظة للمعلم

عناوين IP المخصصة محجوزة لشركة واحدة، لذا لا تختلط حركتها مع المستخدمين الآخرين.

8 تخصيص تقنية المعلومات — مقعد مسؤول تقنية المعلومات — الإجابة الصحيحة: صحيح

ملاحظة للمعلم

تتيح لوحات المعلومات الإدارية المركزية لمديري تقنية المعلومات تخصيص تراخيص المقاعد. المصدر: إرشادات CISA.

9 معيار IPsec — من موقع إلى موقع — الإجابة الصحيحة: خطأ

ملاحظة للمعلم

IPsec هو البروتوكول القياسي المستخدم لأنفاق الفروع بين المواقع. المصدر: IPsec Tunneling.

10 رابط Okta SSO — تسجيل دخول SSO — الإجابة الصحيحة: صحيح

ملاحظة للمعلم

يدمج تسجيل الدخول الموحد عمليات تسجيل الدخول إلى VPN مع أدلة الشركة مثل Okta. المصدر: Okta SSO.

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. انعدام الثقة	D 2. IP مخصص	E 3. IPSEC	G 4. وحدة تحكم المسؤول
B 5. تسجيل الدخول الموحد	C 6. متعدد العوامل	F 7. البوابة	A 8. التوفير

نقطة التحقق 3: مفتاح الإجابة – المصطلحات الأساسية

1 انعدام الثقة	2 عنوان IP مخصص	3 IPsec	4 وحدة التحكم
5 الدخول الموحد	6 متعددة العوامل		

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

1 B – عنوانثابت	2 G – البوابة	3 H – تخصيص	4 F – العوامل
5 C – الانفاق	6 A – الثقة	7 E – الموحد	8 D – وحدةالتحكم

ملاحظات النقاش للمعلمين

المصطلحات الأساسية:
تحقّق من قدرة الطلاب على شرح انعدام الثقة وIP مخصص وIPSEC بكلماتهم الخاصة وإعطاء مثال على كل منها.

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

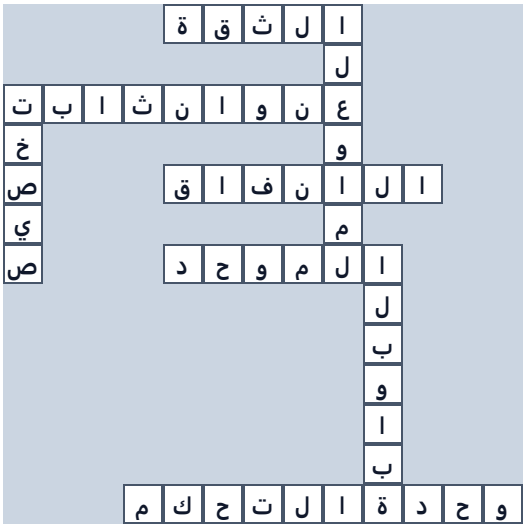
تقييم المصادر:
اطلب من الطلاب التحقق من ادعاء واحد على الأقل من مراجع ورقة العمل، وناقش لماذا قد تتغير الأرقام والأسعار والقواعد مع الوقت.

مفاتيح الألغاز وملاحظات المعلم

حل البحث عن الكلمات

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

حل الكلمات المتقاطعة



دليل المعلم لحلول الكلمات المتقاطعة

أفقي

1 أفقي: الثقة إطار يتحقق منها باستمرار (5 حروف)

2 أفقي: عنوانثابت عنوان بوابة ثابت للقائمة البيضاء (9 حروف)

4 أفقي: الانفاق معيار الاتصال من موقع إلى موقع (IPsec) (7 حروف)

5 أفقي: الموحد ربط الهوية مع Okta وEntra ID (6 حروف)

6 أفقي: وحدةالتحكم بوابة مركزية لمقاعد مدير تقنية المعلومات (10 حروف)

عمودي

1 عمودي: العوامل أمان تسجيل الدخول بطلب رموز إضافية (7 حروف)

3 عمودي: تخصيص منح تراخيص وصول الموظفين إلى VPN (5 حروف)

5 عمودي: البوابة عقدة توجيه مدخل الشبكة (7 حروف)

مفتاح حل الكلمات المبعثرة والشيفرة

مفتاح تصحيح لنشاط فك خلط مفردات المصطلحات وتحدي الشيفرة السرية.

مفتاح ترتيب الكلمات المبعثرة

1. قثاةل ← **الثقة**
2. االقافنل ← **الانفاق**
3. امودحل ← **الموحد**
4. ةلاوباب ← **البوابة**
5. اننثاعبو ← **عنوانثابت**
6. كاةتحوحلمد ← **وحدةالتحكم**
7. اماللوع ← **العوامل**
8. صتصيخ ← **تخصيص**

مفتاح تحدي الشيفرة السرية

"انعدام الثقة يتحقق من الأجهزة المتصلة"

مفتاح إجابات دراسات الحالة

A دراسة الحالة 1: الانتقال إلى انعدام الثقة

حل المعلم

دليل التصحيح

ينبغي أن تغطي إجابات الطلاب النقاط التالية:

- تحليل السيناريو: تريد مؤسسة تأمين خوادمها المحلية عبر التحقق باستمرار من شهادات امتثال الأجهزة وحالة جدار الحماية وموقع المستخدم، بدلًا من الوثوق بأي شخص داخل الشبكة.
- الاستراتيجية والحل الموصى بهما: ينبغي للمدير الانتقال إلى نموذج الوصول إلى الشبكة بدون ثقة (ZTNA)، الذي يفرض فحوصات أمنية مستمرة قائمة على السياق.

B دراسة الحالة 2: تقييد البوابة

حل المعلم

دليل التصحيح

ينبغي أن تغطي إجابات الطلاب النقاط التالية:

- تحليل السيناريو: تستضيف شركة قواعد بيانات مالية خاصة في السحابة. وتريد حظر كل وصول من الإنترنت العام إلى لوحات الإدارة، مع السماح بتسجيل الدخول من نقاط نهاية الشركة الموثقة فقط.
- الاستراتيجية والحل الموصى بهما: ينبغي للمسؤول ضبط بوابة IP مخصص (Dedicated IP) على VPN المؤسسي وإضافة هذا العنوان الثابت إلى القائمة البيضاء في جدار حماية قاعدة البيانات السحابية.