نام: _____ تاریخ: _____ نمره: _____

بهترین VPN برای کسب‌وکار

بررسی عملی امنیت، مقیاس‌پذیری و مدیریت متمرکز VPN کسب‌وکار.

مرور آموزشی بهترین VPN برای کسب‌وکار

یادگیرنده

وضعیت دانشجویی

مسیر مدافع شبکه

امن

وضعیت اتصال

محافظت از بسته‌های داده

فعال

محافظت در برابر نشت

محافظت در برابر نشت DNS و IPv6

خوش آمدید! این بستهٔ فعالیت شما را در بررسی شبکه‌های VPN کسب‌وکار و دسترسی از راه دور راهنمایی می‌کند. با معماری‌های Zero Trust، تونل‌های IPsec سایت‌به‌سایت، چارچوب‌های SASE، ورود چندعاملی و بررسی‌های امنیتی نقطهٔ پایانی آشنا می‌شوید.

ایستگاه‌های بررسی کاربرگ

- ☐ **بخش 1-4: بر پیکربندی‌های VPN و امنیت شبکه مسلط شوید.**
- ☐ **بخش 5-7: جدول‌های متقاطع و جدول‌های جست‌وجوی کلمه را حل کنید.**
- ☐ **بخش 8-9: مطالعات موردی و چالش رمز را حل کنید.**
- ☐ **بخش 10: صفحه‌های پرسش‌های متداول مقدماتی و پیشرفته را مرور کنید.**
- ☐ **بخش 11: 10 واقعیت جالب دنیای واقعی را کاوش کنید.**
- ☐ **تکمیلی: چالش سریع فکر کن**

باز کردن راهنمای بهترین VPNهای VPN.com

URL: https://www.vpn.com/vpn/best-vpn-for-business/

نقشهٔ راه یادگیری VPN کسب‌وکار شما

- بهترین ارائه‌دهندگان VPN کسب‌وکار و ویژگی‌های ویژهٔ تیمی آنها را شناسایی کنید.
- تفاوت‌های حریم خصوصی VPN مصرفی و کنترل‌های مدیریتی کسب‌وکار را تحلیل کنید.
- میان VPNهای دسترسی از راه دور و تونل‌های شرکتی Site-to-Site تمایز قائل شوید.

دستورالعمل راهنمای VPN کسب‌وکار

به پرسش‌های چندگزینه‌ای و درست/نادرست پاسخ دهید، جمله‌های جای‌خالی را با استفاده از بانک واژه‌ها کامل کنید، تعاریف را تطبیق دهید و جدول‌های کلمات متقاطع و جست‌وجوی کلمه را حل کنید. دانسته‌های خود را درباره راه‌اندازی دسترسی از راه دور سازمانی به کار ببرید. و در پایان، فعالیت تکمیلی «سریع فکر کن».

دسترسی از راه دور سازمانی و لبهٔ امن (مقدمه)

ایمن‌سازی دسترسی راه‌دور سازمانی مستلزم گذار از مدل‌های سنتی VPN مبتنی بر محیط پیرامونی به معماری‌های Zero Trust است. اجرای احراز هویت چندعاملی (MFA) قوی و چارچوب‌های Secure Access Service Edge (SASE) از دارایی‌های حساس در برابر نقاط پایانی در معرض خطر محافظت می‌کند.

هر ایستگاه بررسی را با دقت بخوانید و پاسخ درست را انتخاب کنید یا بنویسید.

ایستگاه بررسی 1: چالش چندگزینه‌ای

1. کدام نوع VPN کسب‌وکار شبکه‌های کل دفاتر را به یکدیگر متصل می‌کند؟
   - A. VPN سایت-به-سایت
   - B. VPN دسترسی از راه دور
   - C. VPN مصرفی
   - D. Smart DNS

2. کدام گزینه به‌عنوان بهترین انتخاب کلی برای تیم‌های کسب‌وکار برجسته شده است؟
   - A. NordLayer
   - B. Surfshark
   - C. Proton VPN
   - D. Private Internet Access

3. نشانی IP ثابت اختصاصی برای تیم‌های کسب‌وکار از چه چیزی جلوگیری می‌کند؟
   - A. فهرست سیاه نشانی IP
   - B. سرعت مسیریاب کاهش می‌یابد
   - C. فشرده‌سازی داده
   - D. به‌روزرسانی‌های کلاینت

4. کدام ارائه‌دهنده به‌عنوان بهترین برای زیرساخت اختصاصی برجسته شده است؟
   - A. Proton VPN
   - B. NordLayer
   - C. Surfshark
   - D. Private Internet Access

5. کدام ویژگی یک داشبورد مدیریتی متمرکز برای مدیریت کاربران فراهم می‌کند؟
   - A. کنترل‌های مدیریتی
   - B. ارسال پورت (port forwarding)
   - C. شبیه‌سازی روتر
   - D. تونل‌زنی تفکیکی

ایستگاه بررسی 2: چالش درست یا نادرست

پرسش 6

6. VPNهای دسترسی راه‌دور به کارکنان اجازه می‌دهند از هر جا متصل شوند.

درست نادرست

پرسش 7

7. VPNهای مصرفی از کل یک سازمان را زیر یک پنل مدیریتی واحد محافظت می‌کنند.

درست نادرست

پرسش 8

8. نشانی‌های IP اختصاصی ترافیک شرکت را از ترافیک عمومی جدا نگه می‌دارند.

درست نادرست

پرسش 9

9. Private Internet Access به‌عنوان بهترین گزینه برای سازمان‌های بزرگ معرفی شده است.

درست نادرست

پرسش 10

10. SASE مسیریابی WAN را با چارچوب‌های امنیتی ارائه‌شده از ابر یکپارچه می‌کند.

درست نادرست

ایستگاه بررسی 3: درج اصطلاح کلیدی

هر جملهٔ زیر را بخوانید و جای خالی را با واژهٔ درست از بانک واژگان پر کنید.

1. ارائه‌دهندهٔ رتبه‌اول کلی برای تیم‌های کسب‌وکار _____ است.
2. اتصال چند شعبهٔ شرکتی به یکدیگر از _____ استفاده می‌کند.
3. برای جلوگیری از فهرست سیاه شدن آدرس، تیم‌ها یک _____ به کار می‌گیرند.
4. مدیران مجوزهای دستگاه را با یک _____ مرکزی مدیریت می‌کنند.
5. افزودن پویای صندلی برای پشتیبانی از تیم‌های رو به رشد، _____ است.
6. رعایت استانداردهای مقرراتی و ممیزی داده نیازمند _____ است.

بانک واژگان

آی‌پی ثابت | انطباق | داشبورد | دروازه | سایت‌به‌سایت | مسیریابی | مقیاس‌پذیری | نوردلایر

پاسخ‌های خود را اینجا بنویسید:

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

ایستگاه بررسی 4: تطبیق مفاهیم کلیدی

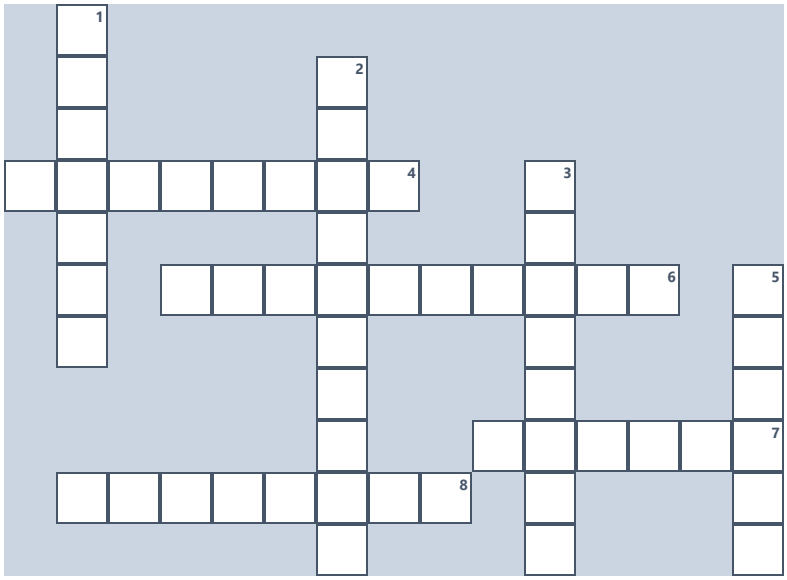
تطبیق تعاریف

هر اصطلاح واژگان در سمت راست را با نوشتن حرف متناظر (A-H) در کادر ورودی قابل‌پرکردن به تعریف درست آن در سمت چپ وصل کنید.

1. NORDLAYER	A	رشد پویای تیم چندجایگاهی.
2. سایت به سایت	B	بهترین انتخاب کلی برای کسب‌وکار.
3. IP ثابت	C	کنترل ترافیک Split tunneling.
4. داشبورد	D	ممیزی استاندارد مقرراتی.
5. مقیاس‌پذیری	E	گرهٔ ورودی راه دور برای احراز هویت.
6. انطباق	F	نشانی اختصاصی بدون فهرست سیاه.
7. مسیریابی	G	تونل ارتباطی میان شبکه‌های دفتر.
8. دروازه	H	کنسول کنترل مدیریتی مرکزی.

ایستگاه بررسی 5: جدول‌کلمات

جدول کلمات متقاطع را با تایپ حروف در خانه‌های سفید فعال حل کنید. شماره‌ها با سرنخ‌های زیر مطابقت دارند.



افقی

4. آدرس اختصاصی بدون سابقهٔ فهرست سیاه (8)

6. تونل اتصال شبکه‌های دفاتر (10)

7. استاندارد ممیزی مقرراتی (6)

8. بهترین گزینهٔ کلی برای کسب‌وکار (8)

عمودی

1. کنسول کنترل مرکزی مدیر (7)

2. رشد پویای تیم با افزودن صندلی (10)

3. کنترل ترافیک در تونل‌زنی تفکیکی (8)

5. گره ورودی راه دور برای احراز هویت (6)

ایستگاه بررسی 5 – فعالیت جایگزین: سرنخ‌های دسترس‌پذیر جدول‌کلمات

کاربران صفحه‌خوان و صفحه‌کلید می‌توانند پاسخ‌های جدول کلمات متقاطع را مستقیماً در فیلدهای متنی زیر تایپ کنند.

افقی

4 افقی: آدرس اختصاصی بدون سابقهٔ فهرست سیاه (8 حرف):

6 افقی: تونل اتصال شبکه‌های دفاتر (10 حرف):

7 افقی: استاندارد ممیزی مقرراتی (6 حرف):

8 افقی: بهترین گزینهٔ کلی برای کسب‌وکار (8 حرف):

عمودی

1 عمودی: کنسول کنترل مرکزی مدیر (7 حرف):

2 عمودی: رشد پویای تیم با افزودن صندلی (10 حرف):

3 عمودی: کنترل ترافیک در تونل‌زنی تفکیکی (8 حرف):

5 عمودی: گره ورودی راه دور برای احراز هویت (6 حرف):

ایستگاه بررسی 6: جدول کلمات پنهان

8 اصطلاح کلیدی واژگان را که در جدول زیر پنهان شده‌اند پیدا کنید. کلمات می‌توانند افقی، عمودی یا مورب باشند.

ک	ف	ق	ج	ژ	ر	پ	ا	ب	پ	ط	و	ژ	ز	و
ژ	ن	ک	ز	ث	ع	ش	ر	ث	ذ	ا	ص	ص	ژ	ع
ظ	خ	ش	ش	ع	غ	ف	ک	ک	خ	ن	پ	ف	ظ	ض
د	ه	د	ر	و	ب	ش	ا	د	ف	ط	پ	م	ث	ق
ت	ز	ه	گ	ت	س	ی	م	ح	ز	ب	خ	ی	م	ث
ب	ا	ص	ث	ع	ا	ن	ن	ظ	پ	ا	گ	ب	س	ا
ا	و	ی	ض	ث	ی	ژ	ا	و	ث	ق	ض	ث	ی	چ
ث	ر	خ	ذ	ث	ت	غ	ع	ش	ر	چ	ذ	ف	ر	ی
ی	د	ق	ج	ع	ب	ل	چ	ا	ا	د	ع	ط	ی	ص
پ	ظ	ک	و	ع	ه	ز	غ	ک	ف	ت	ل	ص	ا	ه
ی	م	ق	ی	ا	س	پ	ذ	ی	ر	ی	پ	ا	ب	ح
ا	ف	ن	م	ر	ا	ا	غ	ی	ه	ه	ژ	ح	ی	ذ
ش	غ	ز	س	س	ی	ق	ط	خ	ظ	ع	خ	ی	ا	ر
ض	ل	ح	گ	پ	ت	ه	ف	ه	ب	خ	س	ی	خ	ز
ض	ظ	ص	ن	پ	س	ی	ه	ح	و	ط	م	گ	ژ	گ

فهرست واژگان

نوردلایر　سایتبهسایت　ایپیثابت　داشبورد　مقیاسپذیری　انطباق　مسیریابی　دروازه

ایستگاه بررسی 6 – فعالیت جایگزین: تطبیق دسترس‌پذیر واژگان

هر یک از 8 اصطلاح واژگان موجود در جدول کلمات پنهان را با نوشتن حرف (A-H) در جای خالی به تعریف درست آن وصل کنید.

اصطلاحات واژگان	تعاریف و فیلدهای تطبیق
A. نوردلایر	1. کنترل ترافیک در تونل‌زنی تفکیکی.
B. سایتبهسایت	2. کنسول کنترل مرکزی مدیر.
C. ایپیثابت	3. گره ورودی راه دور برای احراز هویت.
D. داشبورد	4. آدرس اختصاصی بدون سابقهٔ فهرست سیاه.
E. مقیاسپذیری	5. استاندارد ممیزی مقرراتی.
F. انطباق	6. تونل اتصال شبکه‌های دفاتر.
G. مسیریابی	7. بهترین گزینهٔ کلی برای کسب‌وکار.
H. دروازه	8. رشد پویای تیم با افزودن صندلی.

ایستگاه بررسی 7: چالش کلمات درهم‌ریخته

حروف زیر را مرتب کنید تا مفاهیم کلیدی این کاربرگ آشکار شوند. پاسخ‌هایتان را در کادرهای ورودی ارائه‌شده بنویسید.

1. ی د ل ن ا و ر ر
2. ی ا ت ی ب ا ث پ
3. م پ ر ذ ق س ی ا ی ی
4. ر ب ی ا ی م س ی
5. ا ه ت ا ت س ب س ی ی
6. ر ش و د ب د ا
7. ا ا ب ق ط ن
8. و ه د ز ا ر

فعالیت تکمیلی: سریع فکر کن

برای هر دسته 3 پاسخ بنویسید. هر کس زودتر فهرست را کامل کند برنده است.

1	وعده‌هایی که یک ارائه‌دهندهٔ VPN خوب می‌دهد		
2	چیزهایی که می‌توانند جلسهٔ ویدیویی را مختل کنند		
3	قوانین کار از راه دور ایمن		
4	برنامه‌های اداری که می‌شناسید		
5	چیزهایی که ارائه‌دهندهٔ اینترنت شما می‌تواند ببیند		
6	دلایل دادن VPN به کارمندان		
7	چیزهایی که VPN نمی‌تواند از آن‌ها محافظتتان کند		
8	جاهایی که کارمندان از آن‌ها کار می‌کنند		
9	ابزارهایی که یک شرکت هر روز استفاده می‌کند		
10	روش‌های ورود امن		
11	داده‌هایی که یک شرکت باید محافظت کند		
12	نقش‌ها در بخش فناوری اطلاعات		
13	دستگاه‌هایی که یک کارمند ممکن است داشته باشد		
14	کارهایی که پس از نقض امنیتی باید انجام داد		
15	واژه‌هایی که Zero Trust را توصیف می‌کنند		

ایستگاه بررسی 8: مطالعات موردی VPN و شبکه

مفاهیمی را که آموخته‌اید برای حل سناریوهای واقعی زیر به کار ببرید.

مطالعهٔ موردی 1: فهرست سیاه IP عمومی اشتراکی



سناریو: یک تیم فروش با یک VPN مصرفی به پایگاه‌های داده شرکت دسترسی پیدا می‌کند، اما قفل می‌شود، چون IP خروجی مشترک توسط سامانه‌های ضدکلاهبرداری در فهرست سیاه قرار گرفته است.

پرسش برای بحث: برای رفع این قفل، پیکربندی زیرساخت VPN کسب‌وکار را پیشنهاد دهید.

مطالعهٔ موردی 2: اتصال متقابل دفاتر شرکتی



سناریو: یک شرکت بزرگ با دفاتری در Munich و Boston نیاز دارد سرورهای فایل محلی را بدون عبور ترافیک از فضاهای عمومی وب به‌طور امن به اشتراک بگذارد.

پرسش برای بحث: توپولوژی مناسب VPN کسب‌وکار را انتخاب کنید.

ایستگاه بررسی 9: رمزگشایی

مهندس شبکه کانال‌های مسیریابی و تونل‌های کلاینت را ایمن می‌کند. از کلید حرف-به-عدد زیر استفاده کنید و با نوشتن حرف‌های متناظر در جاهای خالی، پیام را رمزگشایی کنید.

کلید رمزگذاری حرف به عدد

ا=1 ب=2 پ=3 ت=4 ث=5 ج=6 چ=7 ح=8 خ=9 د=10 ذ=11

ر=12 ز=13 ژ=14 س=15 ش=16 ص=17 ض=18 ط=19 ظ=20 ع=21 غ=22

ف=23 ق=24 ک=25 گ=26 ل=27 م=28 ن=29 و=30 ه=31 ی=32

31	25	2	16		12	23	17		10	1	28	4	21	1

29	28	32	1		32	29	1	28	13	1	15

پیام رمزگشایی‌شده:

نکته: هر عدد نشان‌دهندهٔ یک حرف فارسی از کلید بالا است.

ایستگاه بررسی 10: پرسش‌های متداول VPN – مقدماتی (بخش A)

رایج‌ترین پرسش‌ها و پاسخ‌ها دربارهٔ شبکه‌های خصوصی مجازی (VPN) و تونل‌زنی را مرور کنید.

Q1: VPN کسب‌وکار چیست؟

اتصال شبکهٔ امن که به کارکنان راه‌دور و دفاتر اجازه می‌دهد با ایمنی به داده‌های خصوصی شرکت دسترسی داشته باشند.

Q2: VPNهای مصرفی و تجاری چه تفاوتی دارند؟

VPNهای مصرفی مرور شخصی را پنهان می‌کنند؛ VPNهای تجاری با کنسول‌های مدیریت مرکزی از سیستم‌های شرکتی محافظت می‌کنند.

Q3: VPN سایت به سایت چیست؟

تونلی که شبکه‌های کامل دفاتر فیزیکی را از طریق وب به یکدیگر متصل می‌کند.

Q4: VPN دسترسی از راه دور چیست؟

تونلی که به کارکنان راه‌دور مجزا اجازه می‌دهد با ایمنی به شبکهٔ شرکت وصل شوند.

Q5: مزیت IP ثابت اختصاصی چیست؟

ترافیک سازمانی را از مجموعه‌های عمومی جدا نگه می‌دارد و از قرار گرفتن در فهرست سیاه IPهای مشترک جلوگیری می‌کند.

ایستگاه بررسی 10: پرسش‌های متداول VPN – مقدماتی (بخش B)

رایج‌ترین پرسش‌ها و پاسخ‌ها دربارهٔ شبکه‌های خصوصی مجازی (VPN) و تونل‌زنی را مرور کنید.

Q6: کدام ارائه‌دهنده برای کسب‌وکارهای کوچک بهترین است؟

Private Internet Access (PIA)، شناخته‌شده برای مقرون‌به‌صرفه بودن برای تیم‌های کوچک و سادگی راه‌اندازی.

Q7: کدام VPN کسب‌وکار در مجموع رتبهٔ #1 را دارد؟

NordLayer که VPN.com برای قابلیت‌ها و ابزارهای مدیریتی به آن 92/100 داده است.

Q8: مقیاس‌پذیری تیمی در VPNها چیست؟

توانایی افزودن پویای صندلی‌های کاربر، مجوزها و دروازه‌ها با رشد شرکت.

Q9: چرا مدیریت متمرکز حیاتی است؟

به مدیران اجازه می‌دهد سیاست‌های امنیتی را اعمال کنند و دسترسی کارکنان را در یک داشبورد لغو کنند.

Q10: SASE چیست؟

Secure Access Service Edge که مسیریابی WAN را با سرویس‌های امنیتی ارائه‌شده از فضای ابری ادغام می‌کند.

ایستگاه بررسی 10: پرسش‌های متداول VPN – پیشرفته (بخش C)

جنبه‌های فنی پیشرفتهٔ پروتکل‌های تونل‌سازی VPN، یکپارچه‌سازی کلاینت‌های موبایل و استقرار سازمانی را بررسی کنید.

Q1: تونل‌زنی تفکیکی چگونه از تیم‌ها ایمن‌سازی می‌کند؟

ترافیک SaaS خصوصی را داخل تونل امن نگه می‌دارد و دسترسی وب عمومی را به‌صورت محلی مسیریابی می‌کند.

Q2: Proton VPN چه چیزی به کسب‌وکارها ارائه می‌دهد؟

زیرساخت سرور اختصاصی، با امتیاز 88/100 از VPN.com (مستقر در سوئیس).

Q3: کدام استانداردهای انطباق، VPN را الزامی می‌کنند؟

PCI DSS رمزگذاری قوی را در شبکه‌های عمومی الزامی می‌کند؛ HIPAA و GDPR آن را به‌عنوان یک تدبیر حفاظتی انتظار دارند.

Q4: آیا می‌توان VPNهای کسب‌وکار را روی روتر اجرا کرد؟

بله، پیکربندی تونل‌های VPN روی روترها به‌طور خودکار از همهٔ دستگاه‌های اداره محافظت می‌کند.

Q5: احراز هویت چندعاملی چیست؟

الزام چند اعتبارنامه (مانند کارت هوشمند یا کدهای SMS) برای احراز هویت ورودها.

ایستگاه بررسی 10: پرسش‌های متداول VPN – پیشرفته (بخش D)

جنبه‌های فنی پیشرفتهٔ پروتکل‌های تونل‌سازی VPN، یکپارچه‌سازی کلاینت‌های موبایل و استقرار سازمانی را بررسی کنید.

Q6: چرا آدرس‌های IP مشترک در فهرست سیاه قرار می‌گیرند؟

زیرا هزاران کاربر از آن‌ها مشترکاً استفاده می‌کنند و برخی از آن‌ها ممکن است اقدامات مخرب انجام دهند.

Q7: دروازه چگونه کاربران را احراز هویت می‌کند؟

با تأیید گواهی‌های کلاینت، گذرواژه‌ها و کدهای چندعاملی در برابر دایرکتوری‌های فعال.

Q8: Surfshark چه چیزی برای تیم‌ها ارائه می‌دهد؟

بهترین انتخاب VPN.com برای بسته‌های امنیتی، با امتیاز 84/100 و سرورهای فقط-RAM.

Q9: اتصال‌های VPN کسب‌وکار را چگونه ممیزی می‌کنید؟

با بازرسی لاگ‌های اتصال، معیارهای مصرف داده و تاریخچهٔ ورود در کنسول مدیریت.

Q10: کنترل دسترسی اعتماد صفر چیست؟

الگویی که در آن همهٔ دستگاه‌ها نامعتبر فرض می‌شوند و برای هر نشست تأیید لازم است.

بخش 11: 10 واقعیت و بینش دنیای واقعی دربارهٔ VPN

واقعیت‌های دنیای واقعی دربارهٔ سرعت رمزگذاری VPN، ممیزی پروتکل‌ها، اتصال موبایل و کار راه‌دور سازمانی را مرور کنید.

1. بینش VPN

VPN تجاری ترافیک را رمزگذاری می‌کند و سامانه‌های شرکت را از شنود در شبکه‌های عمومی محافظت می‌کند.

2. بینش VPN

VPNهای سایت‌به‌سایت شبکه‌های کامل شعبه‌ها را بدون افشای میزبان‌های محلی به‌صورت ایمن به هم پل می‌زنند.

3. بینش VPN

VPNهای مصرفی مرور شخصی را پنهان می‌کنند، در حالی که VPNهای تجاری دروازه‌های منابع سازمانی را محافظت می‌کنند.

4. بینش VPN

VPN.com به NordLayer امتیاز 92/100 می‌دهد، که بهترین VPN کسب‌وکار در مجموع است.

5. بینش VPN

VPN.com به Proton VPN امتیاز 88/100 می‌دهد و آن را بهترین برای زیرساخت اختصاصی معرفی می‌کند.

6. بینش VPN

VPN.com به Private Internet Access امتیاز 76/100 می‌دهد و آن را بهترین برای تیم‌های کسب‌وکار کوچک رتبه‌بندی می‌کند.

7. بینش VPN

داشبوردهای مدیریتی مرکزی به مسئولان امنیت اجازه می‌دهند مجوزهای کاربران و قوانین دسترسی را مدیریت کنند.

8. بینش VPN

نشانی‌های IP ثابت اختصاصی مانع می‌شوند که تیم‌ها به‌دلیل اشتراک IP با دیگران توسط سامانه‌های کشف تقلب مسدود شوند.

9. بینش VPN

GDPR رمزگذاری را به‌عنوان یک اقدام مناسب برای محافظت از داده‌های شخصی نام می‌برد.

10. بینش VPN

معماری‌های اعتماد صفر همهٔ نقاط پایانی راه دور را، فارغ از موقعیت یا اطلاعات کاربری، راستی‌آزمایی می‌کنند.

منابع و مراجع فنی

راهنمای مطالعه و پازل‌های تعاملی از استانداردها، مشخصات فنی و چارچوب‌های مقرراتی جهانی گردآوری شده‌اند.

منابع علمی و صنعتی

[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/

کلید پاسخ: ایستگاه بررسی 1 – چندگزینه‌ای

1 **توپولوژی تونل** — سایت‌به‌سایت — پاسخ درست: A

نکتهٔ آموزشی

VPNهای سایت‌به‌سایت دفترهای شعبهٔ راه‌دور را به‌صورت کامل و ایمن به یکدیگر وصل می‌کنند. منبع: NIST Zero Trust.

2 **پرسش 2** — پاسخ درست: A

نکتهٔ آموزشی

VPN.com به NordLayer نمرهٔ 92/100 می‌دهد و آن را بهترین گزینهٔ کلی برای تیم‌های کسب‌وکار رتبه‌بندی می‌کند.

3 **فهرست سفید IP** — IP اختصاصی — پاسخ درست: A

نکتهٔ آموزشی

IPهای ثابت اختصاصی مانع می‌شوند که تیم‌ها به‌دلیل فهرست‌های سیاه IP مشترک از دسترسی محروم شوند. منبع: NIST Remote Access.

4 **پرسش 4** — پاسخ درست: A

نکتهٔ آموزشی

VPN.com به Proton VPN نمرهٔ 88/100 می‌دهد و آن را بهترین برای زیرساخت اختصاصی معرفی می‌کند.

5 **کنسول مرکزی** — کنترل‌های مدیریتی — پاسخ درست: A

نکتهٔ آموزشی

پنل‌های متمرکز به مسئولان امنیت اجازه می‌دهند مجوزهای کاربران و صندلی‌ها را مدیریت کنند. منبع: NIST Remote Access.

کلید پاسخ: ایستگاه بررسی 2 – درست یا نادرست

6 **اتصال‌های راه‌دور** — دسترسی از راه دور — پاسخ درست: درست

نکتهٔ آموزشی

VPNهای دسترسی راه‌دور به کارکنان راه‌دور اجازه می‌دهند به سرورهای خصوصی متصل شوند. منبع: NIST Remote Access.

7 **تونل‌های سازمانی** — محدودیت‌های مصرف‌کننده — پاسخ درست: نادرست

نکتهٔ آموزشی

VPNهای مصرفی کنترل‌های مدیریت متمرکز ندارند و برای ممیزی‌های سازمانی مناسب نیستند. منبع: CISA Infrastructure.

8 **جداسازی دروازه** — تونل اختصاصی — پاسخ درست: درست

نکتهٔ آموزشی

IPهای اختصاصی ترافیک شرکت را از شلوغی عمومی جدا می‌کنند تا پایگاه‌های داده ایمن شوند. منبع: NIST Zero Trust.

9 **پرسش 9** — پاسخ درست: نادرست

نکتهٔ آموزشی

VPN.com، PIA (76/100) را بهترین برای کسب‌وکار کوچک می‌داند، نه برای شرکت‌های بزرگ.

10 **ادغام امنیت** — استاندارد SASE — پاسخ درست: درست

نکتهٔ آموزشی

SASE مسیریابی WAN سازمانی را با امنیت اعتماد صفر ارائه‌شده از ابر ادغام می‌کند. منبع: Cloudflare Zero Trust.

کلیدهای واژگان و معیار نمره‌دهی

بارم‌بندی معلم: برای هر تطبیق درست (در مجموع 8 امتیاز) و اصطلاح بافتی (در مجموع 6 امتیاز) 1 امتیاز بدهید.

ایستگاه بررسی 4: کلید پاسخ – تطبیق مفاهیم

B .1 NORDLAYER	G .2 سایت به سایت	F .3 IP ثابت	H .4 داشبورد
A .5 مقیاس‌پذیری	D .6 انطباق	C .7 مسیریابی	E .8 دروازه

ایستگاه بررسی 3: کلید پاسخ – اصطلاحات کلیدی

1 نوردلایر	2 سایت‌به‌سایت	3 آی‌پی ثابت	4 داشبورد
5 مقیاس‌پذیری	6 انطباق		

ایستگاه بررسی 6 – فعالیت جایگزین: کلید پاسخ – تطبیق واژگان

1 G – مسیریابی	2 D – داشبورد	3 H – دروازه	4 C – ایپیثابت
5 F – انطباق	6 B – سایتبهسایت	7 A – نوردلایر	8 E – مقیاسپذیری

یادداشت‌های بحث برای مدرسان

اصطلاحات کلیدی:
بررسی کنید که دانش‌آموزان بتوانند NORDLAYER، سایت به سایت و IP ثابت را با کلمات خودشان توضیح دهند و برای هر کدام مثالی بزنند.

مطالعات موردی:
از دانش‌آموزان بخواهید پیشنهادهای خود را بر پایهٔ واقعیت‌های کاربرگ ارائه کنند، نه نظر شخصی.

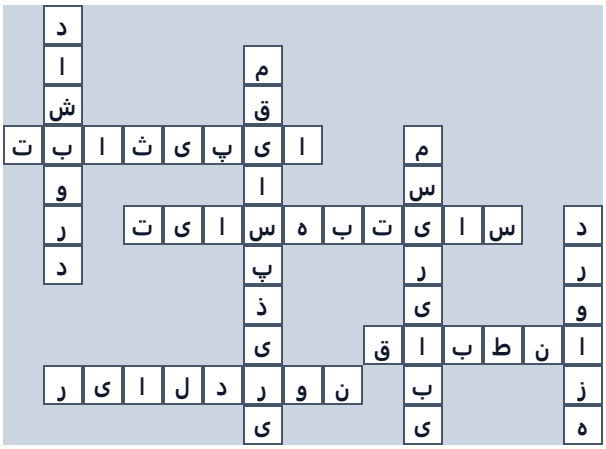
ارزیابی منابع:
از دانش‌آموزان بخواهید دست‌کم یک ادعا را در منابع کاربرگ بررسی کنند و دربارهٔ اینکه چرا ارقام، قیمت‌ها و قوانین ممکن است با گذشت زمان تغییر کنند گفت‌وگو کنید.

کلیدهای معما و یادداشت‌های معلم

پاسخ جدول کلمات

ک	ف	ق	چ	ژ	ر	پ	ا	ب	پ	ط	و	ژ	ز	و
ژ	ن	ک	ز	ث	ع	ش	ر	ث	ذ	ا	س	س	ژ	ع
ظ	خ	ش	ش	ع	غ	ک	ک	خ	ن	پ	ف	ظ	ظ	ض
د	ه	د	ر	و	ب	ش	ا	د	ف	ط	پ	م	ث	ق
ت	ز	ه	گ	ت	س	ی	م	ز	ب	خ	ی	م	ث	ث
ب	ا	س	ث	ع	ا	ن	ن	پ	ا	گ	ب	س	ا	ا
ا	و	ی	ض	ث	ی	ژ	و	ث	ق	ض	ث	ی	چ	چ
ث	ر	خ	ذ	ث	ت	غ	ع	ش	ر	چ	ف	ر	ی	ی
ی	د	ق	چ	ع	ب	ل	ا	ا	د	ع	ط	ی	ص	ص
پ	ظ	ک	و	ع	ه	ز	غ	ف	ت	ل	ص	ا	ه	ه
ی	م	ق	ی	ا	س	پ	ذ	ی	ر	ی	پ	ب	ح	ح
ا	ف	ن	م	ر	ا	ی	غ	ا	ه	ژ	ح	ی	ذ	ذ
ش	غ	ز	س	س	ی	ق	ط	خ	ع	ظ	ی	ا	ر	ر
ض	ل	ح	گ	پ	ت	ه	ف	ب	خ	س	ی	خ	ز	ز
ض	ظ	ص	ن	پ	س	ی	ح	و	ط	م	گ	ژ	گ	گ

پاسخ جدول‌کلمات



راهنمای معلم برای پاسخ‌های جدول کلمات متقاطع

افقی

4 افقی: اپیثابت آدرس اختصاصی بدون سابقهٔ فهرست سیاه (8 حرف)

6 افقی: سایتبهسایت تونل اتصال شبکه‌های دفاتر (10 حرف)

7 افقی: انطباق استاندارد ممیزی مقرراتی (6 حرف)

8 افقی: نوردلایر بهترین گزینهٔ کلی برای کسب‌وکار (8 حرف)

عمودی

1 عمودی: داشبورد کنسول کنترل مرکزی مدیر (7 حرف)

2 عمودی: مقیاسپذیری رشد پویای تیم با افزودن صندلی (10 حرف)

3 عمودی: مسیریابی کنترل ترافیک در تونل‌زنی تفکیکی (8 حرف)

5 عمودی: دروازه گره ورودی راه دور برای احراز هویت (6 حرف)

کلید پاسخ کلمات درهم‌ریخته و رمزگشایی

کلید نمره‌دهی برای فعالیت بازچینی واژگان و چالش رمز مخفی.

کلید مرتب‌سازی کلمات

1. یدلناورر — نوردلایر
2. یاتیباثپ — ایپیثابت
3. مپرذقسیایی — مقیاسپذیری
4. ربیایمسی — مسیریابی
5. اهتاتسبسیی — سایتبهسایت
6. رشودبدا — داشبورد
7. اابقطن — انطباق
8. وهدزار — دروازه

کلید چالش رمز مخفی

"اعتماد صفر شبکه سازمانی ایمن"

کلید پاسخ مطالعات موردی

A مطالعهٔ موردی 1: فهرست سیاه IP عمومی اشتراکی

پاسخ معلم

راهنمای نمره‌دهی

پاسخ‌های دانش‌آموز باید نکات زیر را پوشش دهد:

- تحلیل سناریو: یک تیم فروش با VPN مصرف‌کننده به پایگاه‌های داده سازمانی دسترسی دارد اما چون IP خروجی مشترک توسط سامانه‌های ضدکلاهبرداری در فهرست سیاه قرار گرفته، دسترسی‌اش قفل می‌شود.
- راهبرد و راه‌حل توصیه‌شده: سرورهای اختصاصی کسب‌وکار را همراه با آدرس IP ثابت به کار ببرید تا ترافیک شرکتی از استخرهای عمومی جدا شود.

B مطالعهٔ موردی 2: اتصال متقابل دفاتر شرکتی

پاسخ معلم

راهنمای نمره‌دهی

پاسخ‌های دانش‌آموز باید نکات زیر را پوشش دهد:

- تحلیل سناریو: یک شرکت بزرگ با دفترهایی در مونیخ و بوستون باید سرورهای فایل محلی را بدون عبور ترافیک از فضاهای عمومی وب، به‌صورت ایمن به اشتراک بگذارد.
- راهبرد و راه‌حل توصیه‌شده: یک تونل VPN سایت به سایت پیکربندی کنید تا دو شبکهٔ دفتر محلی را به‌صورت امن از طریق اینترنت به هم متصل کند.