نام: _____ تاریخ: _____ نمره: _____

# VPN سازمانی

پیاده‌سازی دسترسی شبکهٔ اعتماد صفر، گره‌های دروازهٔ اختصاصی و کنترل‌های مدیریتی متمرکز سازمانی.

## مرور یادگیری شبکه‌های VPN سازمانی

**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 سازمانی راهنمایی می‌کند. با معماری‌های اعتماد صفر، دروازه‌های IP ثابت اختصاصی، کنسول‌های مدیر، تأمین منابع و تونل‌های IPsec سایت‌به‌سایت 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/enterprise/

# نقشهٔ راه یادگیری شبکهٔ VPN سازمانی شما

- چارچوب‌های دسترسی شبکهٔ اعتماد صفر (ZTNA) را پیاده‌سازی کنید.
- نشانی‌های IP دروازهٔ سرور اختصاصی را برای فیلترهای فهرست سفید پیکربندی کنید.
- مدیریت پنل‌های مدیریتی متمرکز سازمانی و فهرست صندلی‌های کاربران.
- لاگ‌های دسترسی شبکه و تاریخچهٔ اتصال کاربران را ممیزی کنید.
- قوانین ورود یکپارچه (SSO) و احراز هویت چندعاملی را پیکربندی کنید.
- تونل‌های IPsec سایت‌به‌سایت بین شعبه‌ها را راه‌اندازی کنید.

### دستورالعمل‌های شبکه‌های VPN سازمانی

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 Zero Trust و IPsec سایت‌به‌سایت به کار ببرید. و در پایان، فعالیت تکمیلی «سریع فکر کن».

### معماری‌های اعتماد صفر و دروازه‌های اختصاصی (مقدمه)

VPNهای سازمانی با گذار به چارچوب‌های دسترسی شبکهٔ اعتماد صفر (ZTNA) و فهرست مجاز کردن دروازه‌های IP ثابت اختصاصی، دارایی‌های شرکتی را ایمن می‌کنند. مدیران فناوری اطلاعات از کنسول‌های مدیریت متمرکز برای هماهنگ‌سازی تونل‌های IPsec بین‌سایتی و پیوندهای ورود یکباره (SSO) استفاده می‌کنند.

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

# ایستگاه بررسی 1: چالش چندگزینه‌ای

**1. کدام مدل امنیتی جایگزین VPNهای قدیمی سازمانی می‌شود؟**

- A) Zero Trust
- B) Multi-hop
- C) همتا به همتا
- D) دروازهٔ تکی

**2. برای محدود کردن دسترسی پایگاه داده به سرورهای شرکت کدام ویژگی لازم است؟**

- A) IP اختصاصی
- B) مسیریابی پویا
- C) تونل تقسیم‌شده (Split tunnel)
- D) پراکسی DNS

**3. کدام پروتکل استاندارد تونل‌های سایت‌به‌سایت سازمانی است؟**

- A) IPsec
- B) PPTP
- C) SOCKS5
- D) SSL v3

**4. کدام ابزار مرکزی به مدیران اجازه می‌دهد جایگاه‌های کارکنان را مدیریت کنند؟**

- A) کنسول مدیریت
- B) کلید رجیستری
- C) سفت‌افزار مسیریاب
- D) گزارش سیستم

**5. کدام استاندارد احراز هویت ورود از طریق Okta یا Microsoft Entra ID را ممکن می‌کند؟**

- A) ورود یکپارچه (Single Sign-On)
- B) راز مشترک
- C) احراز هویت EPP
- D) کلید WEP

# ایستگاه بررسی 2: چالش درست یا نادرست

**6 پرسش 6**

6. دسترسی شبکهٔ اعتماد صفر ورود به شبکه را فقط پس از راستی‌آزمایی مداوم اعتماد به دستگاه مجاز می‌کند.

درست نادرست

**7 پرسش 7**

7. دروازه‌های IP اختصاصی ترافیک کارکنان را در کنار کاربران تصادفی عمومی مسیریابی می‌کنند.

درست نادرست

**8 پرسش 8**

8. کنسول‌های مدیریتی متمرکز به مدیران IT اجازه می‌دهند صندلی‌های هر کارمند را فوراً لغو کنند.

درست نادرست

**9 پرسش 9**

9. IPsec یک پروتکل سبک است که از تونل‌های شبکهٔ سایت‌به‌سایت پشتیبانی نمی‌کند.

درست نادرست

**10 پرسش 10**

10. Single Sign-On احراز هویت ایمن کارکنان را با ارائه‌دهندگان هویت سازمانی ممکن 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. معماری‌های امنیتی مدرن تونل‌های قدیمی را با دسترسی _____ جایگزین می‌کنند.
2. برای محدود کردن دسترسی به پایگاه داده، شرکت‌ها یک _____ برای دروازه تنظیم می‌کنند.
3. شعبه‌ها با تونل‌های _____ بین‌سایتی به‌صورت امن متصل می‌شوند.
4. مدیران فناوری اطلاعات مجوزهای کاربری کارکنان را در _____ مرکزی تخصیص می‌دهند.
5. ادغام Okta به کارکنان اجازه می‌دهد از طریق _____ سازمانی احراز هویت کنند.
6. برای محافظت از ورود، پورتال‌های سازمانی احراز هویت _____ را الزامی می‌کنند.

**بانک واژگان**

آی‌پی اختصاصی | اعتماد صفر | تأمین | چندعاملی | دروازه | کنسول مدیریت | ورود واحد | IPsec

**پاسخ‌های خود را اینجا بنویسید:**

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

# ایستگاه بررسی 4: تطبیق مفاهیم کلیدی

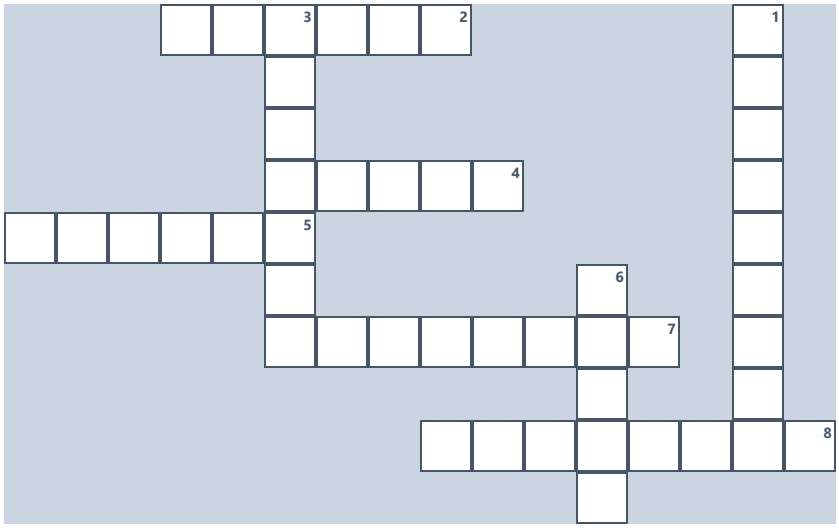
**تطبیق تعاریف**

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. اعتماد صفر | A | تخصیص مجوزهای دسترسی VPN به کارکنان. |
| 2. IP اختصاصی | B | پیوند هویت Okta و Entra ID. |
| 3. IPSEC | C | امنیت ورود که به توکن‌های اضافی نیاز دارد. |
| 4. کنسول مدیریت | D | نشانی دروازهٔ فهرست سفید ایستا. |
| 5. ورود یکپارچه | E | استاندارد تونل سایت‌به‌سایت. |
| 6. چندعاملی | F | گره مسیریابی ورودی شبکه. |
| 7. دروازه | G | درگاه مرکزی صندلی‌های مدیر IT. |
| 8. تأمین | H | چارچوب راستی‌آزمایی مداوم اعتماد. |

# ایستگاه بررسی 5: جدول‌کلمات

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




## افقی

**2. گره مسیریابی ورودی شبکه (6)**

**4. اختصاص مجوزهای دسترسی VPN به کارکنان (5)**

**5. استاندارد تونل بین‌شعبه‌ای (6)**

**7. امنیت ورود که توکن‌های اضافی می‌خواهد (8)**

**8. پیوند هویتی Okta و Entra ID (8)**

## عمودی

**1. چارچوب راستی‌آزمایی مداوم اعتماد (9)**

**3. آدرس دروازهٔ ثابت فهرست سفید (7)**

**6. پورتال مرکزی صندلی مدیر فناوری اطلاعات (5)**

# 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

**2 افقی: گره مسیریابی ورودی شبکه (6 حرف):**

**4 افقی: اختصاص مجوزهای دسترسی VPN به کارکنان (5 حرف):**

**5 افقی: استاندارد تونل بین‌شعبه‌ای (6 حرف):**

**7 افقی: امنیت ورود که توکن‌های اضافی می‌خواهد (8 حرف):**

**8 افقی: پیوند هویتی Okta و Entra ID (8 حرف):**

## عمودی

**1 عمودی: چارچوب راستی‌آزمایی مداوم اعتماد (9 حرف):**

**3 عمودی: آدرس دروازهٔ ثابت فهرست سفید (7 حرف):**

**6 عمودی: پورتال مرکزی صندلی مدیر فناوری اطلاعات (5 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.

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

### فهرست واژگان

اعتمادصفر
اختصاصی
اپیپسک
کنسول
ورودواحد
چندعاملی
دروازه
تخصیص

# 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 |
| --- |
| **A.** اعتمادصفر |
| **B.** اختصاصی |
| **C.** اپیسک |
| **D.** کنسول |
| **E.** ورودواحد |
| **F.** چندعاملی |
| **G.** دروازه |
| **H.** تخصیص |

| تعاریف و فیلدهای تطبیق | |
| --- | --- |
| 1. آدرس دروازهٔ ثابت فهرست سفید. | |
| 2. گره مسیریابی ورودی شبکه. | |
| 3. اختصاص مجوزهای دسترسی VPN به کارکنان. | |
| 4. امنیت ورود که توکن‌های اضافی می‌خواهد. | |
| 5. استاندارد تونل بین‌شعبه‌ای. | |
| 6. چارچوب راستی‌آزمایی مداوم اعتماد. | |
| 7. پیوند هویتی Okta و Entra ID. | |
| 8. پورتال مرکزی صندلی مدیر فناوری اطلاعات. | |

## 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. د ا م ع ا ص ف ر ت
2. ک ا پ س ی ی
3. د ر و و ا د ح و
4. ه ا و ز د ر
5. ا ی ص ت ا ص خ
6. و ک س ل ن
7. چ ی ا م ل ن ع د
8. ص ت ص ی خ

# فعالیت تکمیلی: سریع فکر کن

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

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

# ایستگاه بررسی 8: مطالعات موردی VPN و شبکه

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

### مطالعهٔ موردی 1: مهاجرت به اعتماد صفر



**سناریو:** یک سازمان می‌خواهد با بررسی مداوم گواهی‌های انطباق دستگاه، وضعیت دیوار آتش و موقعیت کاربر، به‌جای اعتماد به هر کسی درون شبکه، سرورهای محلی خود را ایمن کند.

**پرسش برای بحث:** مدیر امنیت فناوری اطلاعات برای دستیابی به این هدف باید چه چارچوبی را پیاده کند؟

### مطالعهٔ موردی 2: محدودسازی دروازه



**سناریو:** یک شرکت پایگاه‌های داده مالی خصوصی را در ابر میزبانی می‌کند. می‌خواهد تمام دسترسی اینترنت عمومی به پنل‌های مدیریت را مسدود کند و ورود را فقط از نقاط انتهایی تأییدشدهٔ شرکت مجاز کند.

**پرسش برای بحث:** مدیر پایگاه داده باید چه پیکربندی شبکه‌ای را روی دیوار آتش ابری تنظیم کند؟

# 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 | 1 | 26 | 4 | 15 | 10 | | 12 | 31 | | 12 | 23 | 17 | | 10 | 1 | 28 | 4 | 21 | 1 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | | | | | |

| 32 | 15 | 12 | 1 | 30 | | 1 | 12 |
|---|---|---|---|---|---|---|---|
| | | | | | | | |

**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 سازمانی چیست؟

تونل شبکهٔ امن طراحی‌شده برای کسب‌وکارها که به کارکنان راه‌دور اجازه می‌دهد با مدیریت متمرکز به شبکه‌های شرکتی دسترسی یابند.

### Q2: اعتماد صفر چه تفاوتی با VPNهای سنتی دارد؟

VPNهای سنتی به هر کس درون تونل اعتماد می‌کنند، در حالی که Zero Trust پیوسته هر اتصال دستگاه و کاربر را راستی‌آزمایی می‌کند.

### Q3: Dedicated IP در VPNهای کسب‌وکار چیست؟

نشانی IP ثابتی که فقط برای کسب‌وکار شما رزرو شده و امکان فهرست مجاز کردن آن را برای دسترسی امن به پایگاه داده ابری فراهم می‌کند.

### Q4: چرا SSO برای VPNهای کسب‌وکار مهم است؟

Single Sign-On به کارکنان اجازه می‌دهد از اطلاعات ورود سازمانی خود (مانند Okta یا Microsoft Entra ID) برای ورود ایمن استفاده کنند.

### Q5: VPN سایت به سایت چیست؟

تونلی که دو دفتر فیزیکی (مانند شعبه و دفتر مرکزی) را با IPsec از طریق اینترنت عمومی به هم وصل 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: کارکرد کنسول مدیریت چیست؟

داشبوردی برای مدیران IT برای افزودن یا حذف صندلی‌های کارکنان، تخصیص دروازه‌ها و پایش اتصال‌های فعال.

### Q7: MFA چگونه VPNهای کسب‌وکار را ایمن می‌کند؟

با الزام به کد ثانویه (مانند توکن برنامهٔ احراز هویت) برای جلوگیری از ورود غیرمجاز با گذرواژه‌های به‌خطرافتاده.

### Q8: آیا می‌توانم تاریخچهٔ اتصال کارکنان را ممیزی کنم؟

بله، VPNهای سازمانی زمان اتصال، مدت و IPهای اختصاص‌یافته را برای ممیزی انطباق ثبت می‌کنند.

### Q9: ZTNA چیست؟

دسترسی شبکهٔ اعتماد صفر، مدلی امنیتی که دسترسی را فقط به برنامه‌های مشخص می‌دهد، نه کل شبکه.

### Q10: نقش گره‌های دروازه چیست؟

آن‌ها به‌عنوان نقاط ورود امن برای ترافیک راه دور عمل می‌کنند و داده‌ها را مستقیماً به سرورهای خصوصی شرکت هدایت می‌کنند.

# 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: IPsec چگونه از ارتباطات شرکتی سایت به سایت محافظت می‌کند؟

IPsec ترافیک را در لایهٔ شبکه با استفاده از Encapsulating Security Payload (ESP) رمزگذاری می‌کند تا محرمانگی و یکپارچگی داده‌ها تضمین شود.

### Q2: چرا امنیت سنتی مبتنی بر محیط پیرامونی برای نیروی کار دورکار شکست می‌خورد؟

زیرا کارکنان از چندین مکان و دستگاه به داده‌ها دسترسی دارند و این موضوع محیط یک دیوار آتش شبکهٔ واحد را منسوخ می‌کند.

### Q3: مدیران فناوری اطلاعات چگونه تأمین خودکار را پیاده‌سازی می‌کنند؟

با نگاشت پروتکل‌های SCIM میان ارائه‌دهندگان هویت (Okta) و کنسول مدیریت VPN برای همگام‌سازی دایرکتوری‌های کاربران.

### Q4: مزیت تونل‌بندی تفکیکی در محیط‌های سازمانی چیست؟

ترافیک SaaS محلی (مانند Microsoft 365) را خارج از تونل VPN مسیریابی می‌کند و پهنای باند دروازهٔ سازمانی را برای پایگاه‌های داده خصوصی حفظ می‌کند.

### Q5: بررسی‌های وضعیت دستگاه چگونه امنیت نقطهٔ پایانی را اعتبارسنجی می‌کنند؟

کلاینت VPN پیش از اتصال دستگاه را اسکن می‌کند تا مطمئن شود دیوار آتش فعال است، آنتی‌ویروس در حال اجراست و وصله‌های سیستم‌عامل به‌روز است.

# 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: نقش NAT traversal در راه‌اندازی VPN کسب‌وکار چیست؟

NAT-T بسته‌های IPsec را درون UDP کپسوله می‌کند تا بدون قطع اتصال از روترها و دیوارهای آتش خانگی عبور کنند.

### Q7: کسب‌وکارها چگونه از گلوگاه پهنای باند دروازه جلوگیری می‌کنند؟

با استقرار چندین گره دروازهٔ منطقه‌ای و متعادل‌سازی ترافیک ورودی کاربران بین آن‌ها با استفاده از متعادل‌کننده‌های بار.

### Q8: چرا فهرست‌های مجاز IP ثابت بر IP پویا ترجیح داده می‌شوند؟

فهرست‌های سفید ایستا از تلاش IPهای بیرونی غیرمجاز برای دست‌دهی اتصال جلوگیری می‌کنند و سطح حمله را به‌طور چشمگیری کاهش می‌دهند.

### Q9: نقش احراز هویت مبتنی بر گواهی در VPNهای سازمانی چیست؟

گواهی‌های دیجیتال یکتای نصب‌شده روی دستگاه‌های تحت مدیریت شرکت را اعتبارسنجی می‌کند و رایانه‌های شخصی مدیریت‌نشده را مسدود می‌کند.

### Q10: ZTNA چگونه خطر حرکت جانبی را کاهش می‌دهد؟

با جداسازی نشست‌های کاربران در منابع مجاز مشخص، که در صورت نفوذ به یک گره مانع از پیمایش شبکه توسط هکرها می‌شود.

# 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

معماری‌های اعتماد صفر وضعیت امنیتی هر دستگاهی را که قصد اتصال به شبکه دارد به‌طور مداوم راستی‌آزمایی می‌کنند.

### 2. بینش VPN

دروازه‌های IP اختصاصی به کسب‌وکارها امکان می‌دهند با فهرست مجاز کردن نشانی‌های ثابت، پایگاه‌های داده ابری را قفل کنند.

### 3. بینش VPN

IPsec پروتکل استاندارد صنعتی برای پیکربندی تونل‌های امن شبکهٔ سایت‌به‌سایت دفاتر است.

### 4. بینش VPN

کنسول‌های مدیریت به بخش‌های IT اجازه می‌دهند صندلی‌های دسترسی VPN کارکنان را تأمین، مدیریت و ممیزی کنند.

### 5. بینش VPN

Single Sign-On دسترسی VPN را با ارائه‌دهندگان هویت سازمانی مانند Okta و Entra ID یکپارچه می‌کند.

### 6. بینش VPN

احراز هویت چندعاملی تلاش‌های اتصال غیرمجاز را که از کلیدهای گذرواژهٔ دزدیده‌شده سرچشمه می‌گیرند مسدود می‌کند.

### 7. بینش VPN

Split tunneling با کنار گذاشتن ترافیک SaaS عمومی از تونل رمزگذاری‌شده، پهنای باند سازمانی را بهینه می‌کند.

### 8. بینش VPN

بررسی‌های وضعیت دستگاه پیش از اعطای دسترسی به سرورهای شرکتی، تنظیمات امنیتی محلی را تأیید می‌کنند.

### 9. بینش VPN

همگام‌سازی دایرکتوری SCIM کنترل‌های دسترسی ورود و خروج کارکنان را خودکار می‌کند.

### 10. بینش VPN

دسترسی شبکهٔ اعتماد صفر دسترسی کاربر را به برنامه‌های مجاز مشخص محدود می‌کند و از حرکت جانبی در شبکه جلوگیری می‌کند.

# 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** **اعتماد صفر** مدل ZTNA — پاسخ درست: **A**

**نکتهٔ آموزشی**

مدل‌های اعتماد صفر انطباق دستگاه را پیش از ورود به شبکه به‌طور مداوم راستی‌آزمایی می‌کنند. منبع: NIST Zero Trust.

**2** **IP اختصاصی** IP ثابت — پاسخ درست: **A**

**نکتهٔ آموزشی**

نشانی‌های IP اختصاصی امکان فهرست مجاز کردن دروازه‌ها را برای مسدود کردن ترافیک عمومی فراهم می‌کنند. منبع: Dedicated IP Guide.

**3** **استاندارد IPsec** تونل IPSEC — پاسخ درست: **A**

**نکتهٔ آموزشی**

IPsec پروتکل استاندارد مورد استفاده برای تونل‌های سایت‌به‌سایت شعب است. منبع: IPsec Tunneling.

**4** **تخصیص فناوری اطلاعات** کنسول مدیریت — پاسخ درست: **A**

**نکتهٔ آموزشی**

داشبوردهای مدیریتی متمرکز به مدیران IT اجازه می‌دهند مجوزهای صندلی را تخصیص دهند. منبع: CISA Guidelines.

**5** **پرسش 5** — پاسخ درست: **A**

**نکتهٔ آموزشی**

کدام استاندارد احراز هویت ورود از طریق Okta یا Microsoft Entra ID را ممکن می‌کند؟ → ورود یکپارچه (Single Sign-On)

## کلید پاسخ: ایستگاه بررسی 2 – درست یا نادرست

**6** اعتماد صفر — بررسی‌های ZTNA — پاسخ درست: درست

### نکتهٔ آموزشی

مدل‌های اعتماد صفر انطباق دستگاه را پیش از ورود به شبکه به‌طور مداوم راستی‌آزمایی می‌کنند. منبع: NIST Zero Trust.

**7** پرسش 7 — پاسخ درست: نادرست

### نکتهٔ آموزشی

IPهای اختصاصی برای یک کسب‌وکار رزرو می‌شوند، بنابراین ترافیک آن با کاربران دیگر مخلوط نمی‌شود.

**8** تخصیص فناوری اطلاعات — صندلی مدیر فناوری اطلاعات — پاسخ درست: درست

### نکتهٔ آموزشی

داشبوردهای مدیریتی متمرکز به مدیران IT اجازه می‌دهند مجوزهای صندلی را تخصیص دهند. منبع: CISA Guidelines.

**9** استاندارد IPsec — سایت‌به‌سایت — پاسخ درست: نادرست

### نکتهٔ آموزشی

IPsec پروتکل استاندارد مورد استفاده برای تونل‌های سایت‌به‌سایت شعب است. منبع: IPsec Tunneling.

**10** پیوند Okta SSO — ورود SSO — پاسخ درست: درست

### نکتهٔ آموزشی

Single Sign-On ورودهای VPN را با دایرکتوری‌های سازمانی مانند Okta یکپارچه می‌کند. منبع: Okta SSO.

# 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

| | | | |
|---|---|---|---|
| H 1. اعتماد صفر | D 2. IP اختصاصی | E 3. IPSEC | G 4. کنسول مدیریت |
| B 5. ورود یکپارچه | C 6. چندعاملی | F 7. دروازه | A 8. تأمین |

## ایستگاه بررسی 3: کلید پاسخ – اصطلاحات کلیدی

| | | | |
|---|---|---|---|
| 1 اعتماد صفر | 2 آی‌پی اختصاصی | 3 IPsec | 4 کنسول مدیریت |
| 5 ورود واحد | 6 چندعاملی | | |

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

| | | | |
|---|---|---|---|
| 1 B – اختصاصی | 2 G – دروازه | 3 H – تخصیص | 4 F – چندعاملی |
| 5 C – ایپیسک | 6 A – اعتمادصفر | 7 E – ورودواحد | 8 D – کنسول |

### یادداشت‌های بحث برای مدرسان

**اصطلاحات کلیدی:**
بررسی کنید که دانش‌آموزان بتوانند اعتماد صفر، IP اختصاصی و IPSEC 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

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

## پاسخ جدول‌کلمات

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | ه | ز | ا | و | ر | د | |
| | | | | | | | | | | | | خ | | | | |
| | | | | | | | | | | | | ت | | | | |
| | | | | | | | | | | | | ص | ی | ص | خ | ت |
| ک | س | ی | پ | ی | ا | | | | | | | | | | | |
| | | | | | | | | | | | | ص | | | | |
| | | | | | | | | | | | | ی | ل | م | ا | ع | د | ن | چ |
| | | | | | | | | | | | | | | | | | | س | |
| | | | | | | | | | | | | | | | | | د | ح | ا | و | د | و | ر | و |
| | | | | | | | | | | | | | | | | | | ل | |

## راهنمای معلم برای پاسخ‌های جدول کلمات متقاطع

### افقی

**2 افقی: دروازه** گره مسیریابی ورودی شبکه (6 حرف)

**4 افقی: تخصیص** اختصاص مجوزهای دسترسی VPN به کارکنان (5 حرف)

**5 افقی: اپیسک** استاندارد تونل بین‌شعبه‌ای (6 حرف)

**7 افقی: چندعاملی** امنیت ورود که توکن‌های اضافی می‌خواهد (8 حرف)

**8 افقی: ورودواحد** پیوند هویتی Okta و Entra ID (8 حرف)

### عمودی

**1 عمودی: اعتمادصفر** چارچوب راستی‌آزمایی مداوم اعتماد (9 حرف)

**3 عمودی: اختصاصی** آدرس دروازهٔ ثابت فهرست سفید (7 حرف)

**6 عمودی: کنسول** پورتال مرکزی صندلی مدیر فناوری اطلاعات (5 حرف)

# کلید پاسخ کلمات درهم‌ریخته و رمزگشایی

کلید نمره‌دهی برای فعالیت بازچینی واژگان و چالش رمز مخفی.

## کلید مرتب‌سازی کلمات

1. دامعاصفرت — اعتمادصفر
2. کاپسیی — ایپیسک
3. درووادحو — ورودواحد
4. هاوزدر — دروازه
5. ایصتاصخ — اختصاصی
6. وکسلن — کنسول
7. چیاملنعد — چندعاملی
8. صتصیخ — تخصیص

### کلید چالش رمز مخفی

**"اعتماد صفر هر دستگاه را وارسی"**

# کلید پاسخ مطالعات موردی

## A مطالعهٔ موردی 1: مهاجرت به اعتماد صفر

پاسخ معلم

### راهنمای نمره‌دهی

**پاسخ‌های دانش‌آموز باید نکات زیر را پوشش دهد:**

- تحلیل سناریو: یک سازمان می‌خواهد با بررسی مداوم گواهی‌های انطباق دستگاه، وضعیت دیوار آتش و موقعیت کاربر، به‌جای اعتماد به هر کسی که داخل شبکه است، سرورهای محلی خود را ایمن کند.
- راهبرد و راه‌حل پیشنهادی: مدیر باید به مدل دسترسی شبکهٔ اعتماد صفر (ZTNA) مهاجرت کند که بررسی‌های امنیتی پیوستهٔ مبتنی بر بافتار را اعمال می‌کند.

## B مطالعهٔ موردی 2: محدودسازی دروازه

پاسخ معلم

### راهنمای نمره‌دهی

**پاسخ‌های دانش‌آموز باید نکات زیر را پوشش دهد:**

- تحلیل سناریو: یک شرکت پایگاه‌های داده مالی خصوصی را در ابر میزبانی می‌کند. می‌خواهد همهٔ دسترسی اینترنت عمومی به پنل‌های مدیریت را مسدود کند و ورود را فقط از نقاط انتهایی تأییدشدهٔ شرکت مجاز کند.
- راهبرد و راه‌حل پیشنهادی: مدیر باید یک دروازهٔ Dedicated IP را روی VPN سازمانی پیکربندی کند و این نشانی ثابت را در دیوار آتش پایگاه داده ابری در فهرست مجاز قرار دهد.