نام: _____ تاریخ: _____ نمبر: _____

# انٹرپرائز VPN

Zero Trust نیٹ ورک رسائی، مخصوص گیٹ وے نوڈز اور مرکزی کارپوریٹ ایڈمن کنٹرولز کا نفاذ۔

## انٹرپرائز VPN نیٹ ورکس کا تعلیمی جائزہ

**سیکھنے والا**
طالب علم کی حیثیت
نیٹ ورک ڈیفینڈر ٹریک

**محفوظ**
کنکشن کی صورتحال
ڈیٹا پیکٹس کی حفاظت

**فعال**
لیک سے تحفظ
DNS اور IPv6 لیک سے تحفظ

**خوش آمدید!** یہ سرگرمی پیکٹ آپ کو انٹرپرائز VPN نیٹ ورکس سے متعارف کراتا ہے۔ آپ Zero Trust آرکیٹیکچرز، مخصوص اسٹیٹک IP گیٹ ویز، ایڈمنسٹریٹر کنسولز، پرووِژننگ، اور سائٹ ٹو سائٹ IPsec ٹنلز کا جائزہ لیں گے۔

**ورک شیٹ کے چیک پوائنٹس**

- ☐ **حصہ 1-4: VPN اور نیٹ ورک سیکیورٹی کنفیگریشنز میں مہارت حاصل کریں۔**
- ☐ **حصہ 5-7: کراس ورڈ اور ورڈ سرچ پہیلیاں حل کریں۔**
- ☐ **حصہ 8-9: کیس اسٹڈیز اور سائفر چیلنج حل کریں۔**
- ☐ **حصہ 10: بنیادی اور اعلیٰ FAQ صفحات کا جائزہ لیں۔**
- ☐ **حصہ 11: 10 دلچسپ حقیقی دنیا کے حقائق دریافت کریں۔**
- ☐ **اضافی: تیزی سے سوچیں چیلنج**

**VPN.com بہترین VPNs گائیڈ کھولیں**

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

# آپ کا انٹرپرائز VPN نیٹ ورک لرننگ روڈ میپ

- Zero Trust Network Access (ZTNA) فریم ورکس نافذ کریں۔
- وائٹ لسٹ فلٹرز کے لیے مخصوص سرور گیٹ وے IP ایڈریسز ترتیب دیں۔
- مرکزی کارپوریٹ ایڈمن پینلز اور صارف سیٹ فہرستوں کا انتظام کریں۔
- نیٹ ورک ایکسیس لاگز اور صارفین کی کنکشن ہسٹری کا آڈٹ کریں۔
- Single Sign-On (SSO) اور ملٹی فیکٹر توثیق کے قواعد ترتیب دیں۔
- برانچ سے برانچ سائٹ ٹو سائٹ IPsec ٹنلز ترتیب دیں۔

### انٹرپرائز VPN نیٹ ورکس کی ہدایات

کثیر انتخابی اور درست/غلط سوالات حل کریں، لفظوں کے ذخیرے کی مدد سے خالی جگہیں پُر کریں، تعریفوں کا ملان کریں، اور کراس ورڈ اور ورڈ سرچ پہیلیاں حل کریں۔ اپنے علم کو زیرو ٹرسٹ اور سائٹ ٹو سائٹ IPsec پر لاگو کریں۔ اور آخر میں اضافی سرگرمی "تیزی سے سوچیں"۔

### زیرو ٹرسٹ آرکیٹیکچرز اور مخصوص گیٹ ویز (تعارف)

انٹرپرائز VPNs کارپوریٹ اثاثوں کو Zero Trust Network Access (ZTNA) فریم ورکس کی طرف منتقلی اور مخصوص جامد IP گیٹ ویز کو وائٹ لسٹ کر کے محفوظ بناتے ہیں۔ IT مینیجرز مرکزی ایڈمن کنسولز کے ذریعے سائٹ ٹو سائٹ IPsec ٹنلز اور سنگل سائن آن (SSO) لنکس کو منظم کرتے ہیں۔

**ہر چیک پوائنٹ کو غور سے پڑھیں اور درست جواب منتخب کریں یا لکھیں۔**

## چیک پوائنٹ 1: کثیر انتخابی چیلنج

1. کون سا سیکیورٹی ماڈل پرانے انٹرپرائز VPNs کی جگہ لے رہا ہے؟
   - A) زیرو ٹرسٹ
   - B) ملٹی ہاپ
   - C) پیئر ٹو پیئر
   - D) واحد گیٹ وے

2. ڈیٹا بیس تک رسائی کو کمپنی کے سرورز تک محدود کرنے کے لیے کون سی خصوصیت درکار ہے؟
   - A) مخصوص IP
   - B) متحرک روٹنگ
   - C) اسپلٹ ٹنل
   - D) DNS پراکسی

3. کارپوریٹ سائٹ ٹو سائٹ ٹنلز کے لیے معیاری پروٹوکول کون سا ہے؟
   - A) IPsec
   - B) PPTP
   - C) SOCKS5
   - D) SSL v3

4. کون سا مرکزی ٹول منتظمین کو ملازمین کی سیٹس کا انتظام کرنے دیتا ہے؟
   - A) ایڈمن کنسول
   - B) رجسٹری کی
   - C) راؤٹر فرم ویئر
   - D) سسٹم لاگ

5. کون سا تصدیقی معیار Okta یا Microsoft Entra ID کے ذریعے لاگ ان کی اجازت دیتا ہے؟
   - A) Single Sign-On
   - B) مشترکہ راز
   - C) EPP تصدیق
   - D) WEP کی

## چیک پوائنٹ 2: درست یا غلط چیلنج

### 6 سوال 6

6. Zero Trust Network Access نیٹ ورک میں داخلہ صرف مسلسل ڈیوائس اعتماد کی تصدیق کے بعد دیتا ہے۔

درست ○ غلط ○

### 7 سوال 7

7. مخصوص IP گیٹ ویز ملازمین کی ٹریفک کو بے ترتیب عوامی صارفین کے ساتھ روٹ کرتے ہیں۔

درست ○ غلط ○

### 8 سوال 8

8. مرکزی ایڈمن کنسولز IT مینیجرز کو انفرادی ملازمین کی سیٹس فوری طور پر منسوخ کرنے دیتے ہیں۔

درست ○ غلط ○

### 9 سوال 9

9. IPsec ایک ہلکا پھلکا پروٹوکول ہے جو سائٹ ٹو سائٹ نیٹ ورک ٹنلز کو سپورٹ نہیں کرتا۔

درست ○ غلط ○

### 10 سوال 10

10. سنگل سائن آن کارپوریٹ شناخت فراہم کنندگان کے ذریعے ملازمین کی محفوظ تصدیق ممکن بناتا ہے۔

درست ○ غلط ○

## چیک پوائنٹ 3: کلیدی اصطلاح شامل کرنا

ذیل میں ہر جملہ پڑھیں اور خالی جگہ کو ورڈ بینک سے درست اصطلاح کے ساتھ پُر کریں۔

1. جدید سیکیورٹی فن تعمیرات پرانی ٹنلز کی جگہ _____ رسائی کا نظام لاتی ہیں۔
2. ڈیٹا بیس تک رسائی محدود کرنے کے لیے کمپنیاں ایک _____ گیٹ وے ایڈریس ترتیب دیتی ہیں۔
3. برانچ دفاتر سائٹ ٹو سائٹ _____ ٹنلز کے ذریعے محفوظ طریقے سے جوڑے جاتے ہیں۔
4. آئی ٹی منتظمین ملازمین کے صارف لائسنس مرکزی _____ کے اندر مختص کرتے ہیں۔
5. Okta انضمام ملازمین کو کارپوریٹ _____ کے ذریعے تصدیق کرنے دیتا ہے۔
6. لاگ اِن کے تحفظ کے لیے انٹرپرائز پورٹلز _____ تصدیق لازمی قرار دیتے ہیں۔

### الفاظ کا بینک

ایڈمن کنسول　آئی پی سیک　پرووِژننگ مخصوص آئی پی　زیرو ٹرسٹ ملٹی فیکٹر　سنگل سائن آن　گیٹ وے

**اپنے جوابات یہاں لکھیں:**

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

# چیک پوائنٹ 4: اہم تصورات کا ملان

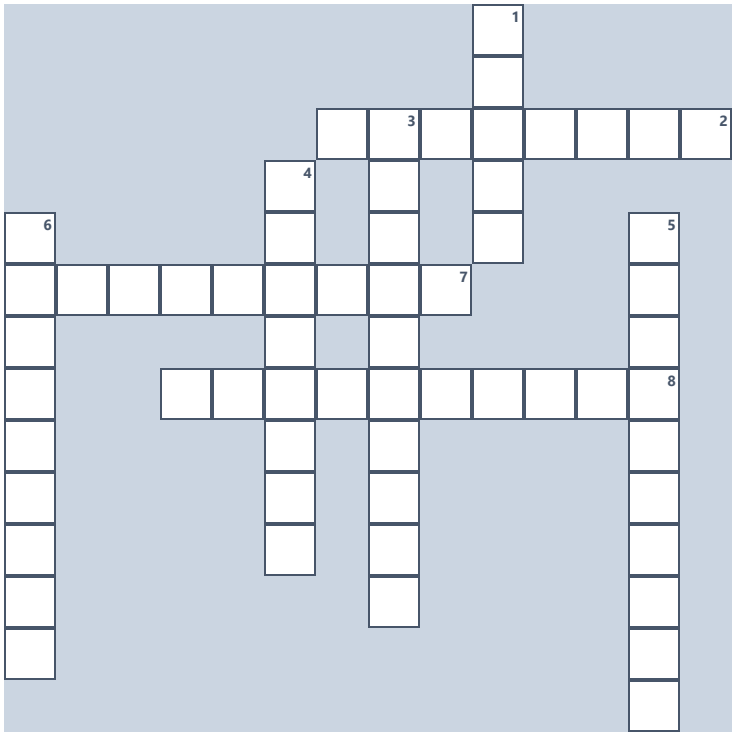
**تعریفوں کا ملان**

دائیں جانب کی ہر اصطلاح کو بائیں جانب کی درست تعریف سے ملائیں اور بھرے جانے والے ان پٹ باکس میں متعلقہ حرف (A-H) لکھیں۔

| | | |
|---|---|---|
| 1. زیرو ٹرسٹ | A | ملازمین کے VPN رسائی لائسنس مختص کرنا۔ |
| 2. مخصوص IP | B | Okta اور Entra ID کی شناختی ربط۔ |
| 3. IPSEC | C | اضافی ٹوکنز کا تقاضا کرنے والی لاگ اِن سیکیورٹی۔ |
| 4. ایڈمن کنسول | D | اسٹیٹک وائٹ لسٹ گیٹ وے ایڈریس۔ |
| 5. سنگل سائن آن | E | سائٹ ٹو سائٹ ٹنل کا معیار۔ |
| 6. ملٹی فیکٹر | F | نیٹ ورک میں داخلے کا روٹنگ نوڈ۔ |
| 7. گیٹ وے | G | مرکزی IT مینیجر سیٹ پورٹل۔ |
| 8. فراہمی | H | مسلسل اعتماد کی تصدیق کا فریم ورک۔ |

# چیک پوائنٹ 5: کراس ورڈ پہیلی

فعال سفید خانوں میں حروف ٹائپ کر کے کراس ورڈ پہیلی حل کریں۔ نمبر نیچے دیے گئے سراغوں سے مطابقت رکھتے ہیں۔



## افقی

**2. مسلسل اعتماد کی تصدیق کا فریم ورک (8)**

**7. لاگ اِن کی ایسی سیکیورٹی جس میں اضافی ٹوکنز درکار ہوں (9)**

**8. جامد وائٹ لسٹ شدہ گیٹ وے ایڈریس (10)**

## عمودی

**1. نیٹ ورک کا داخلی روٹنگ نوڈ (5)**

**3. Okta اور Entra ID کی شناخت کا لنک (10)**

**4. سائٹ ٹو سائٹ ٹنل کا معیار (8)**

**5. آئی ٹی مینیجر کا مرکزی پورٹل (10)**

**6. ملازمین کے VPN رسائی لائسنس مختص کرنا (9)**

# چیک پوائنٹ 5 – متبادل سرگرمی: قابلِ رسائی کراس ورڈ سراغ

اسکرین ریڈر اور کی بورڈ استعمال کرنے والے صارفین نیچے دیے گئے ٹیکسٹ فیلڈز میں کراس ورڈ کے جوابات براہ راست ٹائپ کر سکتے ہیں۔

## افقی

**2 افقی: مسلسل اعتماد کی تصدیق کا فریم ورک (8 حروف):**

**7 افقی: لاگ اِن کی ایسی سیکیورٹی جس میں اضافی ٹوکنز درکار ہوں (9 حروف):**

**8 افقی: جامد وائٹ لسٹ شدہ گیٹ وے ایڈریس (10 حروف):**

## عمودی

**1 عمودی: نیٹ ورک کا داخلی روٹنگ نوڈ (5 حروف):**

**3 عمودی: Okta اور Entra ID کی شناخت کا لنک (10 حروف):**

**4 عمودی: سائٹ ٹو سائٹ ٹنل کا معیار (8 حروف):**

**5 عمودی: آئی ٹی مینیجر کا مرکزی پورٹل (10 حروف):**

**6 عمودی: ملازمین کے VPN رسائی لائسنس مختص کرنا (9 حروف):**

## چیک پوائنٹ 6: پوشیدہ الفاظ کی تلاش

نیچے گرڈ میں چھپی 8 اہم اصطلاحات تلاش کریں۔ الفاظ افقی، عمودی یا ترچھے ہو سکتے ہیں۔

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ز | ے | ے | ٹ | ے | ک | س | ب | پ | ا | ب | پ | ن | ڈ | ک | ش |
| ف | ک | ڈ | ز | ش | ٹ | ہ | ر | ل | ش | ز | ت | ر | ل | ل | ل |
| ل | ک | ہ | و | د | ل | ل | و | ہ | ی | ی | ے | ز | ز | ز | چ |
| و | پ | ے | و | م | ر | ی | و | ب | س | ر | ت | ے | ژ | ز | خ |
| س | ے | پ | ژ | س | م | چ | ی | ش | د | و | ژ | ت | س | س | ل |
| ن | و | ٹ | ہ | ڈ | خ | ژ | و | پ | خ | ٹ | ب | ا | ن | ژ | ژ |
| ک | ٹ | م | ت | ک | س | ا | ن | م | ٹ | ر | م | ٹ | گ | گ | چ |
| ن | ی | د | ر | ت | و | ی | ن | ل | ا | س | ہ | گ | ل | ل | ٹ |
| م | گ | ر | ی | ژ | س | ے | گ | ٹ | ئ | ٹ | ج | ہ | س | س | س |
| ڈ | ج | ا | ا | ہ | ا | ن | ل | ی | ی | و | ز | ڈ | ا | ا | ہ |
| ی | ش | ی | ز | ی | ئ | ت | ل | ف | پ | ف | ب | چ | ئ | ئ | ی |
| ا | ڈ | ئ | س | ا | ی | ی | ژ | ی | ی | ف | ف | ک | ن | ن | چ |
| ر | ل | ہ | ش | گ | پ | گ | ز | ک | س | ن | د | و | ا | ا | ہ |
| د | ژ | ا | ن | س | ی | چ | خ | ٹ | ی | پ | ف | ی | ن | ن | ف |
| ب | د | گ | ژ | چ | ش | م | و | ر | ک | م | ئ | پ | گ | گ | ژ |

### الفاظ کی فہرست

زیروٹرسٹ
مخصوصائیپی
ائیپیسیک
ایڈمنکنسول
پرووِیژننگ
سنگلسائنان
ملٹیفیکٹر
گیٹوے

# چیک پوائنٹ 6 – متبادل سرگرمی: قابلِ رسائی الفاظ کا ملان

ورڈ سرچ کی 8 اصطلاحات میں سے ہر ایک کو اس کی درست تعریف سے ملائیں اور خالی جگہ میں حرف (A-H) لکھیں۔

| اصطلاحات |
| --- |
| **A.** زیروٹرسٹ |
| **B.** مخصوصائیپی |
| **C.** ائیپیسیک |
| **D.** ایڈمنکنسول |
| **E.** سنگلسائنان |
| **F.** ملٹیفیکٹر |
| **G.** گیٹوے |
| **H.** پرووِژننگ |

| تعریفیں اور ملان کے خانے |
| --- |
| 1. جامد وائٹ لسٹ شدہ گیٹ وے ایڈریس۔ |
| 2. نیٹ ورک کا داخلی روٹنگ نوڈ۔ |
| 3. ملازمین کے VPN رسائی لائسنس مختص کرنا۔ |
| 4. لاگ اِن کی ایسی سیکیورٹی جس میں اضافی ٹوکنز درکار ہوں۔ |
| 5. سائٹ ٹو سائٹ ٹنل کا معیار۔ |
| 6. مسلسل اعتماد کی تصدیق کا فریم ورک۔ |
| 7. Okta اور Entra ID کی شناخت کا لنک۔ |
| 8. آئی ٹی مینیجر کا مرکزی پورٹل۔ |

## چیک پوائنٹ 7: الجھے الفاظ کا چیلنج

اس ورک شیٹ کے اہم تصورات ظاہر کرنے کے لیے نیچے دیے گئے حروف کو درست ترتیب میں لائیں۔ اپنے جوابات دیے گئے ان پٹ باکسز میں لکھیں۔

1. س و ٹ ز ر ی ٹ ر
2. پ ا ک ئ ی س ی ی
3. س ا ا ئ ن س ن ل ن گ
4. ٹ ے و گ ی
5. ی ا ی خ و ئ ص م پ ص
6. و ن م ن س ا ی ک ل ڈ
7. ی م ٹ ر ک ی ل ف ٹ
8. گ ی ن پ و ر ژ ن و

# اضافی سرگرمی: تیزی سے سوچیں

ہر زمرے کے لیے 3 جوابات لکھیں۔ جو سب سے پہلے فہرست مکمل کرے وہ جیتتا ہے۔

| | | | |
|---|---|---|---|
| 1 | کمپنی کے روزانہ استعمال ہونے والے ٹولز کے نام | | |
| 2 | وہ چیزیں جو VPN چھپا سکتا ہے | | |
| 3 | آئی ٹی ڈیپارٹمنٹ میں کرداروں کے نام | | |
| 4 | Zero Trust کو بیان کرنے والے الفاظ | | |
| 5 | محفوظ طریقے سے لاگ ان کرنے کے طریقے | | |
| 6 | ملازمین کو VPN دینے کی وجوہات | | |
| 7 | سیکیورٹی خلاف ورزی کے بعد کرنے کے کام | | |
| 8 | سفر کے دوران VPN استعمال کرنے کی وجوہات | | |
| 9 | محفوظ ریموٹ ورک کے اصول | | |
| 10 | وہ ڈیٹا جس کی حفاظت کمپنی پر لازم ہے | | |
| 11 | وہ چیزیں جو ویڈیو میٹنگ میں خلل ڈال سکتی ہیں | | |
| 12 | وہ ڈیوائسز جو VPN استعمال کر سکتی ہیں | | |
| 13 | آپ کے جانے پہچانے آفس پروگرامز کے نام | | |
| 14 | وہ مقامات جہاں سے ملازمین کام کرتے ہیں | | |
| 15 | ملازم کے پاس ہو سکنے والی ڈیوائسز کے نام | | |

# چیک پوائنٹ 8: VPN اور نیٹ ورک کیس اسٹڈیز

جو تصورات آپ نے سیکھے ہیں انہیں نیچے دیے گئے حقیقی منظرناموں کو حل کرنے میں استعمال کریں۔

### کیس اسٹڈی 1: زیرو ٹرسٹ پر منتقلی



**منظرنامہ:** ایک انٹرپرائز اپنے مقامی سرورز کو محفوظ بنانا چاہتا ہے، اس طرح کہ نیٹ ورک کے اندر کسی پر بھی بھروسا کرنے کے بجائے ڈیوائس کمپلائنس سرٹیفیکیٹس، فائر وال کی حالت اور صارف کی لوکیشن کی مسلسل تصدیق کی جائے۔

**بحث کا سوال:** اسے حاصل کرنے کے لیے آئی ٹی سیکیورٹی ڈائریکٹر کو کون سا فریم ورک نافذ کرنا چاہیے؟

### کیس اسٹڈی 2: گیٹ وے کی پابندی



**منظرنامہ:** ایک کمپنی نجی مالیاتی ڈیٹا بیسز کلاؤڈ میں ہوسٹ کرتی ہے۔ وہ ایڈمن پینلز تک عوامی انٹرنیٹ کی تمام رسائی بلاک کرنا چاہتی ہے، اور لاگ ان صرف کمپنی کے تصدیق شدہ اینڈ پوائنٹس سے اجازت دینا چاہتی ہے۔

**بحث کا سوال:** ڈیٹا بیس ایڈمنسٹریٹر کو کلاؤڈ فائر وال پر نیٹ ورک کی کون سی کنفیگریشن سیٹ کرنی چاہیے؟

## چیک پوائنٹ 9: سائفر حل کریں

نیٹ ورک انجینئر روٹنگ چینلز اور کلائنٹ ٹنلز کو محفوظ بناتا ہے۔ نیچے دی گئی حرف سے عدد کی کلید استعمال کر کے خالی جگہوں میں متعلقہ حروف لکھ کر پیغام ڈی کرپٹ کریں۔

**حرف سے عدد خفیہ کاری کی کلید**

ا=1 ب=2 پ=3 ت=4 ٹ=5 ث=6 ج=7 چ=8 ح=9 خ=10 د=11 ڈ=12 ذ=13

ر=14 ڑ=15 ز=16 ژ=17 س=18 ش=19 ص=20 ض=21 ط=22 ظ=23 ع=24 غ=25 ف=26

ق=27 ک=28 گ=29 ل=30 م=31 ن=32 ں=33 و=34 ہ=35 ھ=36 ی=37 ے=38 ئ=39

| 18 | 39 | 1 | 34 | 37 | 12 | | 14 | 35 | | 5 | 18 | 14 | 5 | | 34 | 14 | 37 | 16 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | | | | |

| 1 | 4 | 8 | 32 | 1 | 7 |
|---|---|---|---|---|---|
| | | | | | |

**ڈی کوڈ شدہ پیغام:**

ٹپ: ہر نمبر اوپر دی گئی کلید کے ایک اردو حرف کو ظاہر کرتا ہے۔

# چیک پوائنٹ 10: VPN عمومی سوالات – بنیادی (حصہ A)

ورچوئل پرائیویٹ نیٹ ورکس (VPNs) اور ٹنلنگ کے بارے میں سب سے عام سوالات اور جوابات کا جائزہ لیں۔

### Q1: انٹرپرائز VPN کیا ہے؟

کاروباری اداروں کے لیے بنائی گئی محفوظ نیٹ ورک ٹنل جو ریموٹ کارکنوں کو مرکزی انتظام کے ساتھ کارپوریٹ نیٹ ورکس تک رسائی دیتی ہے۔

### Q2: Zero Trust روایتی VPNs سے کیسے مختلف ہے؟

روایتی VPNs ٹنل کے اندر موجود ہر شخص پر اعتماد کرتے ہیں، جبکہ Zero Trust ہر ڈیوائس اور صارف کے کنکشن کی مسلسل تصدیق کرتا ہے۔

### Q3: کاروباری VPN میں Dedicated IP کیا ہے؟

اسٹیٹک IP ایڈریس جو صرف آپ کے کاروبار کے لیے مخصوص ہے اور محفوظ کلاؤڈ ڈیٹا بیس رسائی کے لیے اسے وائٹ لسٹ کرنے دیتا ہے۔

### Q4: بزنس VPN کے لیے SSO کیوں اہم ہے؟

سنگل سائن آن ملازمین کو اپنی کارپوریٹ اسناد (جیسے Okta یا Microsoft Entra ID) کے ذریعے محفوظ طریقے سے لاگ اِن کرنے کی سہولت دیتا ہے۔

### Q5: سائٹ ٹو سائٹ VPN کیا ہے؟

ایسی ٹنل جو IPsec کے ذریعے عوامی انٹرنیٹ پر دو فزیکل دفاتر (جیسے برانچ آفس اور ہیڈ کوارٹر) کو جوڑتی ہے۔

# چیک پوائنٹ 10: VPN عمومی سوالات – بنیادی (حصہ B)

ورچوئل پرائیویٹ نیٹ ورکس (VPNs) اور ٹنلنگ کے بارے میں سب سے عام سوالات اور جوابات کا جائزہ لیں۔

### Q6: ایڈمن کنسول کا کیا کام ہے؟

IT ایڈمنسٹریٹرز کے لیے ڈیش بورڈ جس سے ملازمین کی سیٹس شامل یا ہٹائی جا سکتی ہیں، گیٹ ویز تفویض کیے جا سکتے ہیں اور فعال کنکشنز کی نگرانی کی جا سکتی ہے۔

### Q7: MFA کاروباری VPN کو کیسے محفوظ بناتا ہے؟

ثانوی کوڈ (جیسے آتھنٹیکیٹر ایپ ٹوکن) درکار کر کے تاکہ سمجھوتہ شدہ پاس ورڈز کے ذریعے غیر مجاز داخلہ روکا جا سکے۔

### Q8: کیا میں ملازمین کی کنکشن ہسٹری کا آڈٹ کر سکتا ہوں؟

ہاں، انٹرپرائز VPNs تعمیل کے آڈٹ کے لیے کنکشن کے ٹائم اسٹیمپ، دورانیہ اور تفویض کردہ IPs لاگ کرتے ہیں۔

### Q9: ZTNA کیا ہے؟

Zero Trust Network Access، ایک سیکیورٹی ماڈل جو پورے نیٹ ورک کے بجائے صرف مخصوص ایپلیکیشنز تک رسائی دیتا ہے۔

### Q10: گیٹ وے نوڈز کا کردار کیا ہے؟

وہ ریموٹ ٹریفک کے لیے محفوظ داخلی مقامات کا کام کرتے ہیں اور ڈیٹا کو براہِ راست نجی کارپوریٹ سرورز تک روٹ کرتے ہیں۔

# چیک پوائنٹ 10: VPN عمومی سوالات – اعلیٰ (حصہ C)

VPN ٹنلنگ پروٹوکولز، موبائل کلائنٹ انضمام اور انٹرپرائز تعیناتی کے جدید تکنیکی پہلوؤں کا جائزہ لیں۔

### Q1: IPsec سائٹ ٹو سائٹ کارپوریٹ مواصلات کا تحفظ کیسے کرتا ہے؟

IPsec ڈیٹا کی رازداری اور سالمیت یقینی بنانے کے لیے Encapsulating Security Payload (ESP) استعمال کرتے ہوئے نیٹ ورک لیئر پر ٹریفک کو خفیہ کرتا ہے۔

### Q2: دور دراز کام کرنے والے عملے کے لیے روایتی پیرامیٹر پر مبنی سیکیورٹی کیوں ناکام ہو رہی ہے؟

کیونکہ ملازمین متعدد مقامات اور ڈیوائسز سے ڈیٹا تک رسائی حاصل کرتے ہیں، جس سے نیٹ ورک کی واحد فائر وال حد بندی متروک ہو جاتی ہے۔

### Q3: IT مینیجرز خودکار پرووِیژننگ کیسے نافذ کرتے ہیں؟

صارف ڈائریکٹریز کو ہم آہنگ کرنے کے لیے شناخت فراہم کنندگان (Okta) اور VPN ایڈمن کنسول کے درمیان SCIM پروٹوکولز کی نقشہ بندی کر کے۔

### Q4: کارپوریٹ ماحول میں اسپلٹ ٹنلنگ کا کیا فائدہ ہے؟

یہ مقامی SaaS ٹریفک (جیسے Microsoft 365) کو VPN ٹنل سے باہر روٹ کرتا ہے، اور کارپوریٹ گیٹ وے کی بینڈوڈتھ نجی ڈیٹا بیسز کے لیے محفوظ رکھتا ہے۔

### Q5: ڈیوائس پوسچر چیکس اینڈ پوائنٹ سیکیورٹی کی توثیق کیسے کرتے ہیں؟

VPN کلائنٹ کنکشن سے پہلے ڈیوائس کو اسکین کر کے تصدیق کرتا ہے کہ فائر وال فعال ہے، اینٹی وائرس چل رہا ہے اور OS پیچز تازہ ترین ہیں۔

# چیک پوائنٹ 10: VPN عمومی سوالات – اعلیٰ (حصہ D)

VPN ٹنلنگ پروٹوکولز، موبائل کلائنٹ انضمام اور انٹرپرائز تعیناتی کے جدید تکنیکی پہلوؤں کا جائزہ لیں۔

**Q6: کاروباری VPN سیٹ اپ میں NAT ٹراورسل کا کیا کردار ہے؟**

NAT-T، IPsec پیکٹس کو UDP میں لپیٹتا ہے تاکہ وہ کنکشن منقطع ہوئے بغیر گھریلو راؤٹرز اور فائر والز سے گزر سکیں۔

**Q7: کاروبار گیٹ وے بینڈوتھ کی رکاوٹ کو کیسے روکتے ہیں؟**

متعدد علاقائی گیٹ وے نوڈز تعینات کر کے اور لوڈ بیلنسرز کے ذریعے آنے والے صارف ٹریفک کو ان کے درمیان تقسیم کر کے۔

**Q8: اسٹیٹک IP وائٹ لسٹس کو ڈائنامک وائٹ لسٹس پر ترجیح کیوں دی جاتی ہے؟**

اسٹیٹک وائٹ لسٹس غیر مجاز بیرونی IPs کو کنکشن ہینڈ شیک کی کوشش سے روکتی ہیں، جس سے حملے کی سطح نمایاں طور پر کم ہو جاتی ہے۔

**Q9: انٹرپرائز VPN میں سرٹیفکیٹ پر مبنی تصدیق کا کیا کردار ہے؟**

یہ کمپنی کے زیر انتظام ڈیوائسز پر انسٹال منفرد ڈیجیٹل سرٹیفکیٹس کی توثیق کرتا ہے، اور غیر منظم ذاتی کمپیوٹرز کو بلاک کرتا ہے۔

**Q10: ZTNA پہلو بہ پہلو نقل و حرکت کا خطرہ کیسے کم کرتا ہے؟**

صارف سیشنز کو مخصوص مجاز وسائل تک الگ رکھ کر، تاکہ کوئی ایک نوڈ متاثر ہونے پر ہیکرز نیٹ ورک میں آگے نہ بڑھ سکیں۔

## حصہ 11: 10 حقیقی دنیا کے VPN حقائق اور بصیرتیں

VPN خفیہ کاری کی رفتار، پروٹوکول آڈٹس، موبائل کنیکٹیویٹی اور انٹرپرائز ریموٹ ورک کے بارے میں حقیقی دنیا کے حقائق کا جائزہ لیں۔

### 1. VPN بصیرت

Zero Trust آرکیٹیکچرز نیٹ ورک کنکشن کی کوشش کرنے والے ہر آلے کی سیکیورٹی حالت کی مسلسل تصدیق کرتے ہیں۔

### 2. VPN بصیرت

مخصوص IP گیٹ ویز کاروباروں کو جامد ایڈریسز وائٹ لسٹ کر کے کلاؤڈ ڈیٹا بیسز کو محفوظ بنانے دیتے ہیں۔

### 3. VPN بصیرت

IPsec محفوظ سائٹ ٹو سائٹ دفتری نیٹ ورک ٹنلز ترتیب دینے کے لیے صنعتی معیار کا پروٹوکول ہے۔

### 4. VPN بصیرت

ایڈمن کنسولز IT شعبوں کو ملازمین کی VPN رسائی سیٹس فراہم کرنے، ان کا انتظام کرنے اور آڈٹ کرنے دیتے ہیں۔

### 5. VPN بصیرت

سنگل سائن آن VPN رسائی کو Okta اور Entra ID جیسے کارپوریٹ شناخت فراہم کنندگان کے ساتھ مربوط کرتا ہے۔

### 6. VPN بصیرت

ملٹی فیکٹر تصدیق چرائی گئی پاس ورڈ کیز سے شروع ہونے والی غیر مجاز کنکشن کوششوں کو بلاک کرتی ہے۔

### 7. VPN کی بصیرت

اسپلٹ ٹنلنگ عوامی SaaS ٹریفک کو خفیہ کردہ ٹنل سے باہر رکھ کر کارپوریٹ بینڈ وڈتھ کو بہتر بناتی ہے۔

### 8. VPN کی بصیرت

ڈیوائس پوسچر چیکس کارپوریٹ سرورز تک رسائی دینے سے پہلے مقامی سیکیورٹی سیٹنگز کی تصدیق کرتے ہیں۔

### 9. VPN کی بصیرت

SCIM ڈائریکٹری سنکرونائزیشن ملازمین کے آن بورڈنگ اور آف بورڈنگ کے رسائی کنٹرولز کو خودکار بناتی ہے۔

### 10. VPN بصیرت

Zero Trust Network Access صارف کی رسائی کو مخصوص مجاز ایپلیکیشنز تک محدود کرتا ہے، جس سے نیٹ ورک میں پہلو بہ پہلو نقل و حرکت رکتی ہے۔

# تکنیکی حوالہ جات اور ماخذ

مطالعاتی گائیڈ اور انٹرایکٹو پہیلیاں عالمی تکنیکی معیارات، تصریحات اور ریگولیٹری فریم ورکس سے مرتب کی گئی ہیں۔

## علمی اور صنعتی حوالہ جات

[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/

## جوابی کلید: چیک پوائنٹ 1 – کثیر انتخابی

**1** زیرو ٹرسٹ — ZTNA ماڈل — درست جواب: **A**

### تدریسی نوٹ

Zero Trust ماڈلز نیٹ ورک میں داخلے سے پہلے ڈیوائس کی تعمیل کی مسلسل تصدیق کرتے ہیں۔ حوالہ: NIST Zero Trust۔

**2** مخصوص IP — اسٹیٹک IP — درست جواب: **A**

### تدریسی نوٹ

مخصوص IP ایڈریسز گیٹ ویز کو وائٹ لسٹ کرنے اور عوامی ٹریفک بلاک کرنے کی سہولت دیتے ہیں۔ حوالہ: Dedicated IP Guide۔

**3** IPsec معیار — IPSEC ٹنل — درست جواب: **A**

### تدریسی نوٹ

IPsec برانچ سائٹ ٹو سائٹ ٹنلز کے لیے استعمال ہونے والا معیاری پروٹوکول ہے۔ حوالہ: IPsec Tunneling۔

**4** IT مختص — ایڈمن کنسول — درست جواب: **A**

### تدریسی نوٹ

مرکزی ایڈمن ڈیش بورڈز IT مینیجرز کو سیٹ لائسنس مختص کرنے دیتے ہیں۔ حوالہ: CISA Guidelines۔

**5** سوال 5 — درست جواب: **A**

### تدریسی نوٹ

کون سا تصدیقی معیار Okta یا Microsoft Entra ID کے ذریعے لاگ ان کی اجازت دیتا ہے؟ → Single Sign-On

## جوابی کلید: چیک پوائنٹ 2 – درست یا غلط

**6** زیرو ٹرسٹ — ZTNA جانچ — درست جواب: درست

### تدریسی نوٹ

Zero Trust ماڈلز نیٹ ورک میں داخلے سے پہلے ڈیوائس کی تعمیل کی مسلسل تصدیق کرتے ہیں۔ حوالہ: NIST Zero Trust۔

**7** سوال 7 — درست جواب: غلط

### تدریسی نوٹ

Dedicated IPs ایک کاروبار کے لیے مخصوص ہوتے ہیں، اس لیے اس کا ٹریفک دوسرے صارفین کے ساتھ مکس نہیں ہوتا۔

**8** IT مختص — IT ایڈمن سیٹ — درست جواب: درست

### تدریسی نوٹ

مرکزی ایڈمن ڈیش بورڈز IT مینیجرز کو سیٹ لائسنس مختص کرنے دیتے ہیں۔ حوالہ: CISA Guidelines۔

**9** IPsec معیار — سائٹ ٹو سائٹ — درست جواب: غلط

### تدریسی نوٹ

IPsec برانچ سائٹ ٹو سائٹ ٹنلز کے لیے استعمال ہونے والا معیاری پروٹوکول ہے۔ حوالہ: IPsec Tunneling۔

**10** Okta SSO لنک — SSO لاگ اِن — درست جواب: درست

### تدریسی نوٹ

سنگل سائن آن VPN لاگ اِنز کو Okta جیسی کارپوریٹ ڈائریکٹریز کے ساتھ مربوط کرتا ہے۔ حوالہ: Okta SSO۔

# الفاظ کی کلید اور درجہ بندی کا معیار

استاد کی گریڈنگ روبرک: ہر درست ملان (کل 8 نمبر) اور سیاقی اصطلاح (کل 6 نمبر) کے لیے 1 نمبر دیں۔

## چیک پوائنٹ 4: جوابی کلید – تصورات کا ملان

| | | | |
|---|---|---|---|
| H 1. زیرو ٹرسٹ | D 2. مخصوص IP | E 3. IPSEC | G 4. ایڈمن کنسول |
| B 5. سنگل سائن آن | C 6. ملٹی فیکٹر | F 7. گیٹ وے | A 8. فراہمی |

## چیک پوائنٹ 3: جوابی کلید – اہم اصطلاحات

| | | | |
|---|---|---|---|
| 1 زیرو ٹرسٹ | 2 مخصوص آئی پی | 3 آئی پی سیک | 4 ایڈمن کنسول |
| 5 سنگل سائن آن | 6 ملٹی فیکٹر | | |

## چیک پوائنٹ 6 – متبادل سرگرمی: جوابی کلید – الفاظ کا ملان

| | | | |
|---|---|---|---|
| 1 B – مخصوصائیپی | 2 G – گیٹوے | 3 H – پرووِژننگ | 4 F – ملٹیفیکٹر |
| 5 C – ائیپیسیک | 6 A – زیروٹرسٹ | 7 E – سنگلسائنان | 8 D – ایڈمنکنسول |

### اساتذہ کے لیے بحث کے نوٹس

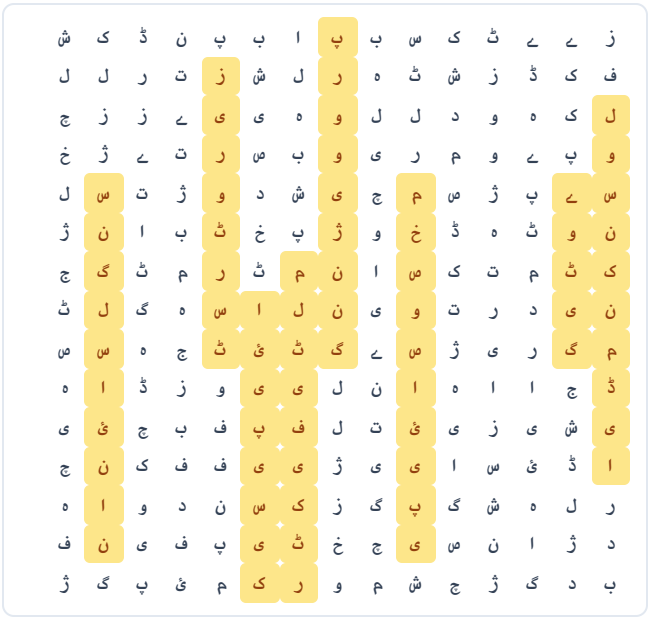
**اہم اصطلاحات:**
یقینی بنائیں کہ طلبہ زیرو ٹرسٹ، مخصوص IP اور IPSEC کو اپنے الفاظ میں سمجھا سکیں اور ہر ایک کی مثال دے سکیں۔

**کیس اسٹڈیز:**
طلبہ سے کہیں کہ اپنی سفارشات کو ورک شیٹ کے حقائق پر مبنی رکھیں، ذاتی رائے پر نہیں۔

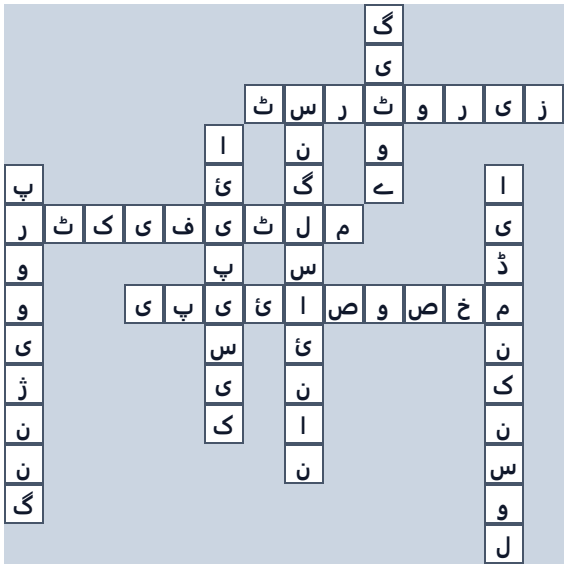
**ماخذ کی جانچ:**
طلبہ سے کہیں کہ ورک شیٹ کے ماخذ میں کم از کم ایک دعوے کی تصدیق کریں، اور اس پر بات کریں کہ اعداد و شمار، قیمتیں اور قواعد وقت کے ساتھ کیوں بدل سکتے ہیں۔

# پہیلیوں کی کلیدیں اور استاد کے نوٹس

## الفاظ کی تلاش کا حل



## کراس ورڈ کا حل



## کراس ورڈ حل کے لیے استاد کی گائیڈ

### افقی

**2 افقی: زیروٹرسٹ** مسلسل اعتماد کی تصدیق کا فریم ورک (8 حروف)

**7 افقی: ملٹیفیکٹر** لاگ اِن کی ایسی سیکیورٹی جس میں اضافی ٹوکنز درکار ہوں (9 حروف)

**8 افقی: مخصوصائیپی** جامد وائٹ لسٹ شدہ گیٹ وے ایڈریس (10 حروف)

### عمودی

**1 عمودی: گیٹوے** نیٹ ورک کا داخلی روٹنگ نوڈ (5 حروف)

**3 عمودی: سنگلسائنان** Okta اور Entra ID کی شناخت کا لنک (10 حروف)

**4 عمودی: ائیپیسیک** سائٹ ٹو سائٹ ٹنل کا معیار (8 حروف)

**5 عمودی: ایڈمنکنسول** آئی ٹی مینیجر کا مرکزی پورٹل (10 حروف)

**6 عمودی: پروویژننگ** ملازمین کے VPN رسائی لائسنس مختص کرنا (9 حروف)

# الفاظ کی ترتیب اور سائفر حل کی کلید

الفاظ کی ترتیب درست کرنے کی سرگرمی اور Secret Cipher Challenge کی گریڈنگ کلید۔

## الفاظ کی ترتیب درست کرنے کی کلید

1. سوٹزریٹر — زیروٹرسٹ
2. پاکئیسیی — ائیپیسیک
3. سااٹنسلنگ — سنگلسائنان
4. ٹےوگی — گیٹوے
5. یایخوئصمپص — مخصوصائیپی
6. ونمنسایکلڈ — ایڈمنکنسول
7. یمٹرکیلفٹ — ملٹیفیکٹر
8. گینپورژنو — پرووِیژننگ

### خفیہ سائفر چیلنج کی کلید

**"زیرو ٹرسٹ ہر ڈیوائس جانچتا"**

# کیس اسٹڈیز کی جوابی کلید

## A کیس اسٹڈی 1: زیرو ٹرسٹ پر منتقلی

استاد کا حل

### گریڈنگ کی ہدایت

**طلبہ کے جوابات میں درج ذیل نکات شامل ہونے چاہییں:**

- منظرنامے کا تجزیہ: ایک انٹرپرائز اپنے مقامی سرورز کو محفوظ بنانا چاہتی ہے، اور نیٹ ورک کے اندر موجود کسی پر بھی بھروسا کرنے کے بجائے ڈیوائس کمپلائنس سرٹیفکیٹس، فائر وال کی حالت اور صارف کے مقام کی مسلسل تصدیق کرنا چاہتی ہے۔
- تجویز کردہ حکمت عملی اور حل: ڈائریکٹر کو زیرو ٹرسٹ نیٹ ورک ایکسیس (ZTNA) ماڈل پر منتقل ہونا چاہیے، جو مسلسل سیاق و سباق پر مبنی سیکیورٹی جانچ نافذ کرتا ہے۔

## B کیس اسٹڈی 2: گیٹ وے کی پابندی

استاد کا حل

### گریڈنگ کی ہدایت

**طلبہ کے جوابات میں درج ذیل نکات شامل ہونے چاہییں:**

- منظرنامے کا تجزیہ: ایک کمپنی کلاؤڈ میں نجی مالیاتی ڈیٹا بیسز ہوسٹ کرتی ہے۔ وہ ایڈمن پینلز تک تمام عوامی انٹرنیٹ رسائی بلاک کرنا چاہتی ہے اور لاگ اِنز کی اجازت صرف تصدیق شدہ کمپنی اینڈ پوائنٹس سے دینا چاہتی ہے۔
- تجویز کردہ حکمت عملی اور حل: ایڈمنسٹریٹر کو انٹرپرائز VPN پر Dedicated IP گیٹ وے ترتیب دینا چاہیے اور اس مستقل ایڈریس کو کلاؤڈ ڈیٹا بیس فائر وال پر وائٹ لسٹ کرنا چاہیے۔