नाम: _____ दिनांक: _____ अंक: _____

# बिज़नेस के लिए सर्वश्रेष्ठ VPN

बिज़नेस VPN की सुरक्षा, स्केलेबिलिटी और केंद्रीय प्रशासन की हैंड्स-ऑन समीक्षा।

## बिज़नेस के लिए सर्वश्रेष्ठ VPN सीखने का अवलोकन

**शिक्षार्थी**
**छात्र का दर्जा**
नेटवर्क डिफ़ेंडर ट्रैक

**सुरक्षित**
**कनेक्शन की स्थिति**
डेटा पैकेट की ढाल बनाना

**सक्रिय**
**लीक सुरक्षा**
DNS और IPv6 लीक सुरक्षा

**स्वागत है!** यह गतिविधि पैकेट आपको बिज़नेस VPN और रिमोट एक्सेस नेटवर्क से परिचित कराता है। आप Zero Trust आर्किटेक्चर, IPsec साइट-टू-साइट टनल, SASE फ़्रेमवर्क, मल्टी-फ़ैक्टर लॉगिन और एंडपॉइंट सुरक्षा जाँच का अध्ययन करेंगे।

**वर्कशीट चेकपॉइंट**

- [ ] **भाग 1-4: VPN और नेटवर्क सुरक्षा कॉन्फ़िगरेशन में महारत हासिल करें।**
- [ ] **भाग 5-7: क्रॉसवर्ड और वर्ड सर्च पहेलियाँ हल करें।**
- [ ] **भाग 8-9: केस स्टडी और कूट संदेश की चुनौती हल करें।**
- [ ] **भाग 10: बुनियादी और उन्नत FAQ पेज देखें।**
- [ ] **भाग 11: 10 रोचक वास्तविक तथ्यों को जानें।**
- [ ] **अतिरिक्त: झटपट सोचें चुनौती।**

**VPN.com सर्वश्रेष्ठ VPN गाइड खोलें**

URL: https://www.vpn.com/hi/vpn/business-ke-liye-best-vpn/

# आपका बिज़नेस VPN लर्निंग रोडमैप

- शीर्ष बिज़नेस VPN प्रदाताओं और उनकी टीम-विशिष्ट सुविधाओं की पहचान करें।
- उपभोक्ता VPN गोपनीयता और व्यावसायिक प्रशासनिक नियंत्रणों के बीच अंतर का विश्लेषण करें।
- रिमोट एक्सेस VPN और साइट-टू-साइट कॉर्पोरेट टनल में अंतर करें।

## बिज़नेस VPN गाइड निर्देश

बहुविकल्पीय और सही/गलत प्रश्नों के उत्तर दें, शब्द बैंक की मदद से रिक्त स्थान भरें, परिभाषाओं का मिलान करें, और क्रॉसवर्ड तथा वर्ड सर्च पहेलियाँ हल करें। अपने ज्ञान को एंटरप्राइज़ रिमोट एक्सेस सेटअप पर लागू करें। अंत में अतिरिक्त गतिविधि झटपट सोचें पूरी करें।

## एंटरप्राइज़ रिमोट एक्सेस और सुरक्षित एज (परिचय)

कॉर्पोरेट रिमोट एक्सेस को सुरक्षित करने के लिए पारंपरिक परिधि-आधारित VPN मॉडल से ज़ीरो ट्रस्ट आर्किटेक्चर की ओर बढ़ना ज़रूरी है। मज़बूत मल्टी-फ़ैक्टर ऑथेंटिकेशन (MFA) और Secure Access Service Edge (SASE) फ़्रेमवर्क लागू करना संवेदनशील परिसंपत्तियों को समझौता किए गए एंडपॉइंट से बचाता है।

**प्रत्येक चेकपॉइंट को ध्यान से पढ़ें और सही उत्तर चुनें या लिखें।**

# चेकपॉइंट 1: बहुविकल्पीय चुनौती

1. किस प्रकार का बिज़नेस VPN पूरे ऑफ़िस नेटवर्क को एक-दूसरे से जोड़ता है?
   - A. साइट-टू-साइट VPN
   - B. रिमोट एक्सेस VPN
   - C. उपभोक्ता VPN
   - D. Smart DNS

2. बिज़नेस टीमों के लिए कुल मिलाकर सबसे अच्छा विकल्प कौन-सा चुना गया है?
   - A. NordLayer
   - B. Surfshark
   - C. Proton VPN
   - D. Private Internet Access

3. डेडिकेटेड स्टैटिक IP पता बिज़नेस टीमों के लिए किस चीज़ को रोकता है?
   - A. IP पता ब्लैकलिस्टिंग
   - B. राउटर की गति घट जाती है
   - C. डेटा कंप्रेशन
   - D. क्लाइंट अपडेट

4. समर्पित इंफ्रास्ट्रक्चर के लिए सबसे अच्छा प्रदाता कौन-सा चुना गया है?
   - A. Proton VPN
   - B. NordLayer
   - C. Surfshark
   - D. Private Internet Access

5. कौन-सी सुविधा उपयोगकर्ताओं को प्रबंधित करने के लिए केंद्रीकृत एडमिन डैशबोर्ड देती है?
   - A. एडमिन नियंत्रण
   - B. पोर्ट फ़ॉरवर्डिंग
   - C. राउटर एमुलेशन
   - D. स्प्लिट टनलिंग

# चेकपॉइंट 2: सही या गलत चुनौती

**6 प्रश्न 6**

6. रिमोट एक्सेस VPN अलग-अलग कर्मचारियों को कहीं से भी जुड़ने देते हैं।

○ सही ○ गलत

**7 प्रश्न 7**

7. उपभोक्ता VPN एक एडमिन पैनल के अंतर्गत पूरे संगठन की सुरक्षा करते हैं।

○ सही ○ गलत

**8 प्रश्न 8**

8. डेडिकेटेड IP पते कंपनी के ट्रैफ़िक को सार्वजनिक ट्रैफ़िक से अलग रखते हैं।

○ सही ○ गलत

**9 प्रश्न 9**

9. Private Internet Access को बड़े उद्यमों के लिए सर्वश्रेष्ठ बताया गया है।

○ सही ○ गलत

**10 प्रश्न 10**

10. SASE, WAN रूटिंग को क्लाउड से दी जाने वाली सुरक्षा फ़्रेमवर्क के साथ जोड़ता है।

○ सही ○ गलत

## चेकपॉइंट 3: मुख्य शब्द भरें

नीचे दिए गए प्रत्येक वाक्य को पढ़ें और रिक्त स्थान को वर्ड बैंक के सही शब्द से भरें।

1. व्यावसायिक टीमों में डिवाइस और सीटों का प्रबंधन आमतौर पर आईटी _____ करते हैं।

2. कई कॉर्पोरेट शाखा कार्यालयों को आपस में जोड़ने के लिए _____ का उपयोग होता है।

3. कर्मचारियों के डिवाइस से कंपनी नेटवर्क तक डेटा सुरक्षित पहुंचाने के लिए _____ का उपयोग होता है।

4. कंपनी के संसाधनों को बाहरी खतरों से बचाने का काम _____ का हिस्सा है।

5. केवल अधिकृत कर्मचारियों को नेटवर्क में आने देने के लिए सख्त _____ लागू किया जाता है।

6. नियामकीय ऑडिट के लिए कंपनी नेटवर्क के _____ रिकॉर्ड और निगरानी ज़रूरी हो सकती है।

**शब्दावली शब्द-बैंक**

टनलिंग ट्रैफ़िक डैशबोर्ड नेटवर्क सुरक्षा प्रमाणीकरण प्रशासक साइट-टू-साइट स्केलेबिलिटी

**अपने उत्तर यहाँ लिखें:**

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

# चेकपॉइंट 4: प्रमुख अवधारणा मिलान

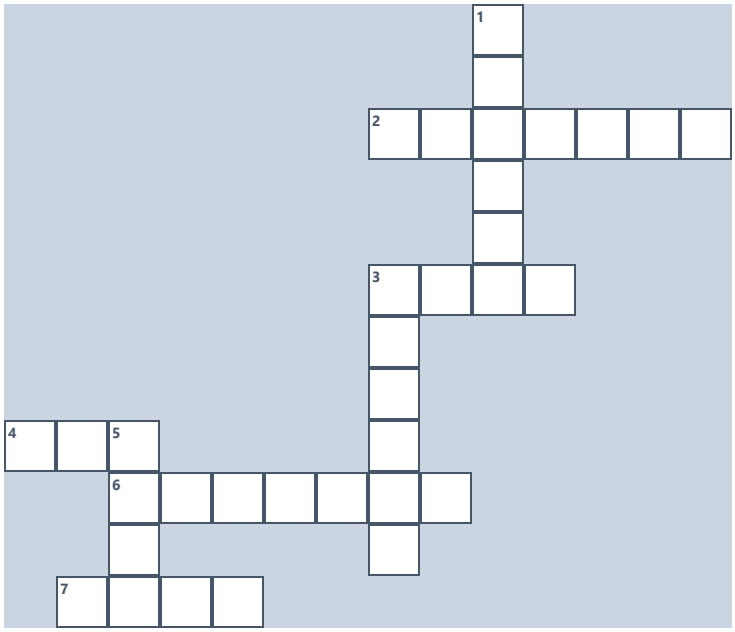
### परिभाषा मिलान

बाईं ओर के प्रत्येक शब्दावली पद को दाईं ओर की सही परिभाषा से मिलाएँ; भरने योग्य इनपुट बॉक्स में संबंधित अक्षर (A-H) लिखें।

| | | | |
|---|---|---|---|
| ☐ | **1. NordLayer** | **A** | डायनामिक मल्टी-सीट टीम वृद्धि। |
| ☐ | **2. साइट-टू-साइट** | **B** | कुल मिलाकर सर्वश्रेष्ठ बिज़नेस विकल्प। |
| ☐ | **3. स्टैटिक IP** | **C** | स्प्लिट टनलिंग ट्रैफ़िक नियंत्रण। |
| ☐ | **4. डैशबोर्ड** | **D** | नियामकीय ऑडिट का मानक ऑडिट। |
| ☐ | **5. स्केलेबिलिटी** | **E** | ऑथेंटिकेशन रिमोट एंट्री नोड। |
| ☐ | **6. अनुपालन** | **F** | समर्पित, ब्लैकलिस्ट में न आया हुआ पता। |
| ☐ | **7. रूटिंग** | **G** | कार्यालय नेटवर्क को जोड़ने वाली टनल। |
| ☐ | **8. गेटवे** | **H** | केंद्रीय एडमिन नियंत्रण कंसोल। |

# चेकपॉइंट 5: क्रॉसवर्ड पहेली

सक्रिय सफ़ेद खानों में अक्षर टाइप करके क्रॉसवर्ड पहेली हल करें। संख्याएँ नीचे दिए गए संकेतों से मेल खाती हैं।




## बाएँ से दाएँ

**2. कार्यालय नेटवर्क को आपस में जोड़ने वाली टनल (7)**

**3. वह व्यक्ति, जो संगठन के सिस्टम, खातों और अनुमतियों का प्रबंधन करता है (4)**

**4. नेटवर्क पर एक साथ आने-जाने वाला सारा डेटा (3)**

**6. नेटवर्क और उसके डेटा को अनधिकृत पहुंच और हमलों से बचाने के उपायों का समूह (7)**

**7. सुरक्षित ट्रांज़िट के लिए डेटा पैकेटों को किसी दूसरे पैकेट के भीतर लपेटना (4)**

## ऊपर से नीचे

**1. दूर बैठे कर्मचारी का कंपनी नेटवर्क और संसाधनों तक सुरक्षित रूप से पहुंचना (6)**

**3. यह जांचने की प्रक्रिया कि लॉगिन करने वाला उपयोगकर्ता वास्तव में वही है जो वह होने का दावा करता है (6)**

**5. डिवाइस और सर्वर या नेटवर्क के बीच बना संपर्क, जिससे डेटा का आदान-प्रदान होता है (4)**

# चेकपॉइंट 5, वैकल्पिक: सुलभ क्रॉसवर्ड संकेत

स्क्रीन-रीडर और कीबोर्ड उपयोगकर्ता क्रॉसवर्ड के उत्तर सीधे नीचे दिए गए टेक्स्ट फ़ील्ड में टाइप कर सकते हैं।

## बाएँ से दाएँ

**2 बाएँ से दाएँ: कार्यालय नेटवर्क को आपस में जोड़ने वाली टनल (7 अक्षर):**

**3 बाएँ से दाएँ: वह व्यक्ति, जो संगठन के सिस्टम, खातों और अनुमतियों का प्रबंधन करता है (4 अक्षर):**

**4 बाएँ से दाएँ: नेटवर्क पर एक साथ आने-जाने वाला सारा डेटा (3 अक्षर):**

**6 बाएँ से दाएँ: नेटवर्क और उसके डेटा को अनधिकृत पहुंच और हमलों से बचाने के उपायों का समूह (7 अक्षर):**

**7 बाएँ से दाएँ: सुरक्षित ट्रांज़िट के लिए डेटा पैकेटों को किसी दूसरे पैकेट के भीतर लपेटना (4 अक्षर):**

## ऊपर से नीचे

**1 ऊपर से नीचे: दूर बैठे कर्मचारी का कंपनी नेटवर्क और संसाधनों तक सुरक्षित रूप से पहुंचना (6 अक्षर):**

**3 ऊपर से नीचे: यह जांचने की प्रक्रिया कि लॉगिन करने वाला उपयोगकर्ता वास्तव में वही है जो वह होने का दावा करता है (6 अक्षर):**

**5 ऊपर से नीचे: डिवाइस और सर्वर या नेटवर्क के बीच बना संपर्क, जिससे डेटा का आदान-प्रदान होता है (4 अक्षर):**

## चेकपॉइंट 6: छिपे शब्द खोजें

नीचे दी गई ग्रिड में छिपे 8 प्रमुख शब्दावली शब्द खोजें। शब्द क्षैतिज, ऊर्ध्वाधर या तिरछे हो सकते हैं।

सा स स ई ते घ इ नी ल रि द जे घ छ ई
के क्से द प ति के ट मि प्र ट सा य च ऊ नी
जी ए इ त म पे ब प जि शा मी ने ले इ सी
य ट छ र दे कि जा सा वा ड स रे स ख नि
फ मो ढ मा ना सा का रे दे सि मी क क पि ता
ति रि ज श भ इ ऊ ने अ ऊ ए क ने क्श न
ण क फ़ि ट्रै रि ट वि श ट य वि व वा पा ल
र च से कि य टू घ प न व के की व सि री
क त की कि सि सा ना ने लिं पा र्क ते ण ए ता
णी सा मी न नी इ ऋ ले ग घ ति सु जि ला ए
मा जी ले ड ल ट द जे घ के च से र दे री
प्र ए पी उ अ जे मि घ व आ च मी च क्षा ट
थ फ ग ना सी का ज फ नी जी ता ठ से लि ट
आ इ से रा के री पा वा सि य नि पि ने ख के
वे ऊ ड नी दे दि भ आ नि जे वे वे ष ण प

**शब्दावली शब्द-सूची**

साइटटूसाइट, प्रशासक, कनेक्शन, नेटवर्कसुरक्षा, ट्रैफ़िक, टनलिंग, रिमोटएक्सेस, प्रमाणीकरण

# चेकपॉइंट 6, वैकल्पिक: सुलभ शब्दावली मिलान

वर्ड सर्च के 8 शब्दावली पदों में से प्रत्येक को उसकी सही परिभाषा से मिलाएँ; खाली स्थान में अक्षर (A-H) लिखें।

| शब्दावली के शब्द |
|---|
| **A. साइटटूसाइट** |
| **B. प्रशासक** |
| **C. कनेक्शन** |
| **D. नेटवर्कसुरक्षा** |
| **E. ट्रैफ़िक** |
| **F. टनलिंग** |
| **G. रिमोटएक्सेस** |
| **H. प्रमाणीकरण** |

| परिभाषाएँ और मिलान फ़ील्ड | |
|---|---|
| | 1. दूर बैठे कर्मचारी का कंपनी नेटवर्क और संसाधनों तक सुरक्षित रूप से पहुंचना। |
| | 2. नेटवर्क और उसके डेटा को अनधिकृत पहुंच और हमलों से बचाने के उपायों का समूह। |
| | 3. यह जांचने की प्रक्रिया कि लॉगिन करने वाला उपयोगकर्ता वास्तव में वही है जो वह होने का दावा करता है। |
| | 4. डिवाइस और सर्वर या नेटवर्क के बीच बना संपर्क, जिससे डेटा का आदान-प्रदान होता है। |
| | 5. सुरक्षित ट्रांज़िट के लिए डेटा पैकेटों को किसी दूसरे पैकेट के भीतर लपेटना। |
| | 6. वह व्यक्ति, जो संगठन के सिस्टम, खातों और अनुमतियों का प्रबंधन करता है। |
| | 7. कार्यालय नेटवर्क को आपस में जोड़ने वाली टनल। |
| | 8. नेटवर्क पर एक साथ आने-जाने वाला सारा डेटा। |

## चेकपॉइंट 7: उलझे शब्दों की चुनौती

नीचे के अक्षरों को सुलझाकर इस वर्कशीट की प्रमुख अवधारणाएँ पता करें। अपने उत्तर दिए गए इनपुट बॉक्स में लिखें।

1. **टू इ सा सा ट ट इ** _____

2. **क क्श न ने** _____

3. **क फ़ि ट्रै** _____

4. **स ए ट क्से रि मो** _____

5. **क प्र स शा** _____

6. **र व सु ने र्क क्षा ट** _____

7. **लिं ट ग न** _____

8. **णी ण प्र र क मा** _____

# अतिरिक्त गतिविधि: झटपट सोचें

हर श्रेणी में 3 उत्तर। जो सबसे पहले सूची भर दे, वह जीतता है।

| | | | | |
|---|---|---|---|---|
| 1 | अच्छे VPN प्रदाता के वादे | | | |
| 2 | वीडियो मीटिंग में बाधा डालने वाली चीज़ें | | | |
| 3 | सुरक्षित रिमोट वर्क के नियम | | | |
| 4 | आपके जाने-पहचाने ऑफ़िस प्रोग्राम | | | |
| 5 | ऐसी चीज़ें जो आपका इंटरनेट प्रदाता देख सकता है | | | |
| 6 | कर्मचारियों को VPN देने के कारण | | | |
| 7 | ऐसी चीज़ें जिनसे VPN आपको नहीं बचा सकता | | | |
| 8 | ऐसी जगहें जहाँ से कर्मचारी काम करते हैं | | | |
| 9 | ऐसे टूल जिन्हें कोई कंपनी रोज़ इस्तेमाल करती है | | | |
| 10 | सुरक्षित रूप से लॉग इन करने के तरीके | | | |
| 11 | ऐसा डेटा जिसे कंपनी को सुरक्षित रखना होता है | | | |
| 12 | IT विभाग की भूमिकाएँ | | | |
| 13 | ऐसे डिवाइस जो किसी कर्मचारी के पास हो सकते हैं | | | |
| 14 | सुरक्षा उल्लंघन के बाद की जाने वाली चीज़ें | | | |
| 15 | Zero Trust का वर्णन करने वाले शब्द | | | |

# चेकपॉइंट 8: VPN और नेटवर्क केस स्टडी

नीचे दिए गए वास्तविक परिदृश्यों को हल करने के लिए सीखी हुई अवधारणाओं का उपयोग करें।

## केस स्टडी 1: साझा सार्वजनिक IP का ब्लैकलिस्ट होना

👷

**परिदृश्य:** एक सेल्स टीम कंज़्यूमर VPN के ज़रिए कॉर्पोरेट डेटाबेस तक पहुँचती है, लेकिन लॉकआउट हो जाती है क्योंकि साझा एग्ज़िट IP को फ़्रॉड सिस्टम ने ब्लैकलिस्ट कर दिया था।

**चर्चा प्रश्न:** इस लॉक को सुलझाने के लिए एक बिज़नेस VPN इन्फ्रास्ट्रक्चर कॉन्फ़िगरेशन सुझाइए।

## केस स्टडी 2: कॉर्पोरेट कार्यालयों का इंटरकनेक्शन

👷

**परिदृश्य:** म्यूनिख और बोस्टन में कार्यालयों वाली एक उद्यम कंपनी को सार्वजनिक वेब स्थानों पर ट्रैफ़िक भेजे बिना स्थानीय फ़ाइल सर्वर सुरक्षित रूप से साझा करने होते हैं।

**चर्चा प्रश्न: उपयुक्त बिज़नेस VPN टोपोलॉजी चुनें।**

# चेकपॉइंट 9: कूट संदेश को डिकोड करें

नेटवर्क इंजीनियर रूटिंग चैनलों और क्लाइंट टनल को सुरक्षित करता है। नीचे दी गई अक्षर-से-संख्या कुंजी का उपयोग करके संदेश को डिक्रिप्ट करें और खाली स्थानों में मेल खाते अक्षर लिखें।

**अक्षर-से-संख्या एन्क्रिप्शन कुंजी**

अ=1 आ=2 इ=3 ई=4 उ=5 ऊ=6 ऋ=7 ए=8 ऐ=9 ओ=10 औ=11 ऑ=12
क=13 ख=14 ग=15 घ=16 ङ=17 च=18 छ=19 ज=20 झ=21 ञ=22 ट=23 ठ=24
ड=25 ढ=26 ण=27 त=28 थ=29 द=30 ध=31 न=32 प=33 फ=34 ब=35 भ=36
म=37 य=38 र=39 ल=40 व=41 श=42 ष=43 स=44 ह=45 ा=46 ि=47 ी=48
ु=49 ू=50 ृ=51 े=52 ै=53 ो=54 ौ=55 ॉ=56 ं=57 ँ=58 ः=59 ़=60
्=61

20 60 48 39 54 23 61 39 44 61 23

8 57 23 39 33 61 39 46 3 20 60 32 52 23 41 39 61 13

35 18 46 28 46

## डिकोड किया गया संदेश:

सुझाव: हर संख्या वर्णमाला में उस अक्षर की स्थिति दर्शाती है (जैसे 1 = अ, 2 = आ, 61 = ्)।

# चेकपॉइंट 10: बुनियादी VPN FAQ (भाग A)

वर्चुअल प्राइवेट नेटवर्क (VPN) और टनलिंग से जुड़े सबसे आम सवाल और जवाब देखें।

**Q1: बिज़नेस VPN क्या है?**
सुरक्षित नेटवर्क कनेक्शन जो दूरस्थ स्टाफ़ और कार्यालयों को निजी कॉर्पोरेट डेटा तक सुरक्षित रूप से पहुँचने देता है।

**Q2: उपभोक्ता और बिज़नेस VPN में क्या अंतर है?**
उपभोक्ता VPN निजी ब्राउज़िंग को छिपाते हैं; बिज़नेस VPN केंद्रीय एडमिन कंसोल के साथ कॉर्पोरेट सिस्टम की सुरक्षा करते हैं।

**Q3: Site-to-Site VPN क्या है?**
टनल जो पूरे भौतिक कार्यालय नेटवर्क को वेब पर एक-दूसरे से जोड़ती है।

**Q4: Remote Access VPN क्या है?**
टनल जो अलग-अलग दूरस्थ कर्मचारियों को कंपनी नेटवर्क से सुरक्षित रूप से जुड़ने देती है।

**Q5: डेडिकेटेड स्टैटिक IP का क्या लाभ है?**
यह कॉर्पोरेट ट्रैफ़िक को सार्वजनिक पूल से अलग रखता है और साझा IP ब्लैकलिस्टिंग से बचाता है।

# चेकपॉइंट 10: बुनियादी VPN FAQ (भाग B)

वर्चुअल प्राइवेट नेटवर्क (VPN) और टनलिंग से जुड़े सबसे आम सवाल और जवाब देखें।

### Q6: छोटे व्यवसायों के लिए कौन-सा प्रदाता सबसे अच्छा है?

Private Internet Access (PIA), जो छोटी टीमों के लिए किफ़ायती होने और आसान सेटअप के लिए जाना जाता है।

### Q7: कुल मिलाकर कौन-सा बिज़नेस VPN #1 रैंक पर है?

NordLayer, जिसे VPN.com ने सुविधाओं और एडमिन टूल के लिए 92/100 का स्कोर दिया।

### Q8: VPN में टीम स्केलेबिलिटी क्या है?

कंपनी के बढ़ने के साथ उपयोगकर्ता सीटें, लाइसेंस और गेटवे गतिशील रूप से जोड़ पाने की क्षमता।

### Q9: केंद्रीय प्रबंधन महत्वपूर्ण क्यों है?

यह एडमिन को एक ही डैशबोर्ड में सुरक्षा नीतियाँ लागू करने और कर्मचारी एक्सेस रद्द करने देता है।

### Q10: SASE क्या है?

Secure Access Service Edge, जो WAN रूटिंग को क्लाउड से दी जाने वाली सुरक्षा सेवाओं के साथ जोड़ता है।

# चेकपॉइंट 10: उन्नत VPN FAQ (भाग C)

VPN टनलिंग प्रोटोकॉल, मोबाइल क्लाइंट एकीकरण और एंटरप्राइज़ तैनाती के उन्नत तकनीकी पहलुओं को जानें।

### Q1: स्प्लिट टनलिंग टीमों को कैसे सुरक्षित करती है?

यह निजी SaaS ट्रैफ़िक को सुरक्षित टनल के भीतर रखता है, जबकि सार्वजनिक वेब एक्सेस को स्थानीय रूप से रूट करता है।

### Q2: Proton VPN व्यवसायों को क्या देता है?

डेडिकेटेड सर्वर इन्फ़्रास्ट्रक्चर, जिसे VPN.com (स्विट्ज़रलैंड-आधारित) ने 100 में से 88 अंक दिए।

### Q3: कौन-से अनुपालन मानक VPN की माँग करते हैं?

PCI DSS सार्वजनिक नेटवर्क पर मज़बूत एन्क्रिप्शन की माँग करता है; HIPAA और GDPR इसे एक सुरक्षा उपाय के रूप में अपेक्षित मानते हैं।

### Q4: क्या आप राउटर पर बिज़नेस VPN चला सकते हैं?

हाँ, राउटर पर VPN टनल कॉन्फ़िगर करने से ऑफ़िस के सभी डिवाइस अपने-आप सुरक्षित हो जाते हैं।

### Q5: मल्टी-फ़ैक्टर ऑथेंटिकेशन क्या है?

लॉगिन प्रमाणित करने के लिए कई क्रेडेंशियल (जैसे स्मार्ट कार्ड या SMS कोड) माँगना।

# चेकपॉइंट 10: उन्नत VPN FAQ (भाग D)

VPN टनलिंग प्रोटोकॉल, मोबाइल क्लाइंट एकीकरण और एंटरप्राइज़ तैनाती के उन्नत तकनीकी पहलुओं को जानें।

### Q6: साझा IP पते ब्लैकलिस्ट क्यों हो जाते हैं?

क्योंकि हज़ारों उपयोगकर्ता उन्हें साझा करते हैं, जिनमें से कुछ दुर्भावनापूर्ण गतिविधियाँ कर सकते हैं।

### Q7: गेटवे उपयोगकर्ताओं को कैसे प्रमाणित करता है?

सक्रिय डायरेक्टरी के विरुद्ध क्लाइंट प्रमाणपत्र, पासवर्ड और मल्टी-फ़ैक्टर कोड सत्यापित करके।

### Q8: Surfshark टीमों को क्या देता है?

VPN.com की सुरक्षा बंडलों के लिए सर्वश्रेष्ठ पसंद, 84/100 अंक के साथ, जिसमें केवल-RAM सर्वर हैं।

### Q9: आप बिज़नेस VPN कनेक्शन का ऑडिट कैसे करते हैं?

एडमिन कंसोल में कनेक्शन लॉग, डेटा उपयोग मेट्रिक्स और लॉगिन इतिहास की जाँच करके।

### Q10: Zero Trust एक्सेस कंट्रोल क्या है?

ऐसी सोच जिसमें सभी उपकरणों को अविश्वसनीय माना जाता है और हर सत्र के लिए सत्यापन ज़रूरी होता है।

# भाग 11: 10 वास्तविक VPN तथ्य और अंतर्दृष्टियाँ

VPN एन्क्रिप्शन की गति, प्रोटोकॉल ऑडिट, मोबाइल कनेक्टिविटी और एंटरप्राइज़ रिमोट वर्क से जुड़े वास्तविक तथ्य देखें।

**1. VPN इनसाइट**

बिज़नेस VPN ट्रैफ़िक को एन्क्रिप्ट करता है और कंपनी के सिस्टम को सार्वजनिक नेटवर्क पर स्निफ़िंग से बचाता है।

**2. VPN इनसाइट**

साइट-टू-साइट VPN स्थानीय होस्ट को उजागर किए बिना पूरे ब्रांच नेटवर्क को सुरक्षित रूप से जोड़ते हैं।

**3. VPN इनसाइट**

उपभोक्ता VPN निजी ब्राउज़िंग को छिपाते हैं, जबकि बिज़नेस VPN एंटरप्राइज़ संसाधन गेटवे की सुरक्षा करते हैं।

**4. VPN इनसाइट**

VPN.com NordLayer को 92/100 अंक देता है, जो इसका सर्वश्रेष्ठ समग्र बिज़नेस VPN है।

**5. VPN इनसाइट**

VPN.com Proton VPN को 88/100 अंक देता है और इसे समर्पित इन्फ्रास्ट्रक्चर के लिए सर्वश्रेष्ठ बताता है।

**6. VPN इनसाइट**

VPN.com Private Internet Access को 76/100 अंक देता है और इसे छोटी बिज़नेस टीमों के लिए सर्वश्रेष्ठ बताता है।

**7. VPN इनसाइट**

केंद्रीय एडमिन डैशबोर्ड सुरक्षा अधिकारियों को उपयोगकर्ता अनुमतियाँ और एक्सेस नियम प्रबंधित करने देते हैं।

**8. VPN इनसाइट**

समर्पित स्थिर IP पते टीमों को IP साझा करने वाले धोखाधड़ी-रोधी सिस्टमों द्वारा ब्लॉक होने से बचाते हैं।

**9. VPN इनसाइट**

GDPR एन्क्रिप्शन को व्यक्तिगत डेटा की सुरक्षा के लिए एक उचित उपाय के रूप में नामित करता है।

**10. VPN इनसाइट**

ज़ीरो ट्रस्ट आर्किटेक्चर स्थान या क्रेडेंशियल की परवाह किए बिना सभी रिमोट एंडपॉइंट को सत्यापित करते हैं।

# तकनीकी संदर्भ और स्रोत

यह अध्ययन गाइड और इंटरैक्टिव पहेलियाँ वैश्विक तकनीकी मानकों, विनिर्देशों और नियामक ढाँचों से तैयार की गई हैं।

## शैक्षणिक और उद्योग संदर्भ

[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/

## उत्तर कुंजी: चेकपॉइंट 1 – बहुविकल्पीय

**1** **टनल टोपोलॉजी** साइट-टू-साइट **सही उत्तर: A**

### शिक्षण नोट

साइट-टू-साइट VPN पूरे दूरस्थ ब्रांच कार्यालयों को आपस में सुरक्षित रूप से जोड़ते हैं। उद्धरण: NIST Zero Trust।

**2** **प्रश्न 2** **सही उत्तर: A**

### शिक्षण नोट

VPN.com, NordLayer को 92/100 अंक देता है और उसे बिज़नेस टीमों के लिए सर्वश्रेष्ठ समग्र विकल्प रेट करता है।

**3** **IP व्हाइटलिस्टिंग** डेडिकेटेड IP **सही उत्तर: A**

### शिक्षण नोट

समर्पित स्थिर IP साझा IP ब्लैकलिस्ट के कारण टीमों के लॉक आउट होने से बचाते हैं। उद्धरण: NIST Remote Access।

**4** **प्रश्न 4** **सही उत्तर: A**

### शिक्षण नोट

VPN.com, Proton VPN को 88/100 अंक देता है और उसे डेडिकेटेड इन्फ्रास्ट्रक्चर के लिए सर्वश्रेष्ठ बताता है।

**5** **केंद्रीय कंसोल** एडमिन नियंत्रण **सही उत्तर: A**

### शिक्षण नोट

केंद्रीकृत पैनल सुरक्षा अधिकारियों को उपयोगकर्ता अनुमतियाँ और सीटें प्रबंधित करने देते हैं। उद्धरण: NIST Remote Access।

## उत्तर कुंजी: चेकपॉइंट 2 – सही या गलत

**6** **रिमोट कनेक्शन** रिमोट एक्सेस — **सही उत्तर: सही**

### शिक्षण नोट

रिमोट एक्सेस VPN अलग-अलग रिमोट कर्मचारियों को निजी सर्वरों से जुड़ने देते हैं। उद्धरण: NIST Remote Access।

**7** **एंटरप्राइज़ टनल** उपभोक्ता सीमाएँ — **सही उत्तर: गलत**

### शिक्षण नोट

उपभोक्ता VPN में केंद्रीकृत एडमिन नियंत्रण नहीं होते और वे संगठन ऑडिट के लिए उपयुक्त नहीं हैं। उद्धरण: CISA Infrastructure।

**8** **गेटवे आइसोलेशन** डेडिकेटेड टनल — **सही उत्तर: सही**

### शिक्षण नोट

डेडिकेटेड IP कंपनी के ट्रैफ़िक को सार्वजनिक शोर से अलग करके डेटाबेस को सुरक्षित रखते हैं। उद्धरण: NIST Zero Trust।

**9** **प्रश्न 9** — **सही उत्तर: गलत**

### शिक्षण नोट

VPN.com, PIA (76/100) को छोटे व्यवसाय के लिए सर्वश्रेष्ठ रेट करता है, बड़े उद्यमों के लिए नहीं।

**10** **सुरक्षा विलय** SASE मानक — **सही उत्तर: सही**

### शिक्षण नोट

SASE एंटरप्राइज़ WAN रूटिंग को क्लाउड से दी जाने वाली ज़ीरो-ट्रस्ट सुरक्षा के साथ मिलाता है। उद्धरण: Cloudflare Zero Trust।

# शब्दावली कुंजियाँ और ग्रेडिंग रूब्रिक

**शिक्षक के लिए ग्रेडिंग रूब्रिक: हर सही मिलान (कुल 8 अंक) और संदर्भ शब्द (कुल 6 अंक) के लिए 1 अंक दें।**

## चेकपॉइंट 4: उत्तर – अवधारणा मिलान

| | | | |
|---|---|---|---|
| B 1. NordLayer | G 2. साइट-टू-साइट | F 3. स्टैटिक IP | H 4. डैशबोर्ड |
| A 5. स्केलेबिलिटी | D 6. अनुपालन | C 7. रूटिंग | E 8. गेटवे |

## चेकपॉइंट 3: उत्तर – प्रमुख शब्द

| | | | |
|---|---|---|---|
| 1 प्रशासक | 2 साइट-टू-साइट | 3 टनलिंग | 4 नेटवर्क सुरक्षा |
| 5 प्रमाणीकरण | 6 ट्रैफ़िक | | |

## चेकपॉइंट 6, वैकल्पिक: उत्तर – शब्द मिलान

| | | | |
|---|---|---|---|
| 1 G – रिमोटएक्सेस | 2 D – नेटवर्कसुरक्षा | 3 H – प्रमाणीकरण | 4 C – कनेक्शन |
| 5 F – टनलिंग | 6 B – प्रशासक | 7 A – साइटटूसाइट | 8 E – ट्रैफ़िक |

## शिक्षकों के लिए चर्चा नोट

**प्रमुख शब्द:**
जाँचें कि क्या विद्यार्थी NordLayer, साइट-टू-साइट और स्टैटिक IP को अपने शब्दों में समझा सकते हैं और हर एक का उदाहरण दे सकते हैं।

**केस स्टडी:**
विद्यार्थियों से कहें कि वे अपनी सिफ़ारिशें राय के बजाय वर्कशीट के तथ्यों पर आधारित करें।

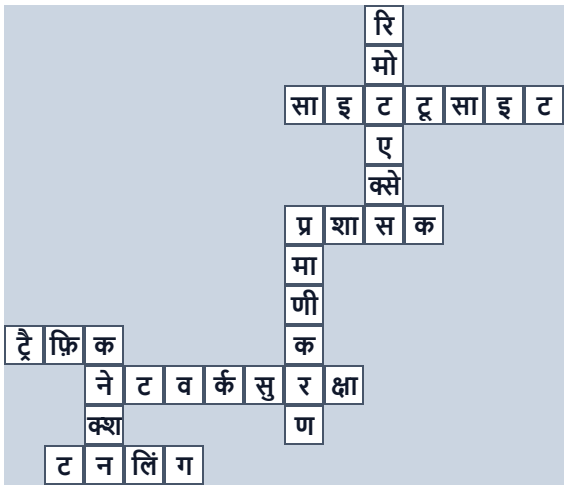
**स्रोतों का मूल्यांकन:**
विद्यार्थियों से वर्कशीट के स्रोतों में कम से कम एक कथन की पुष्टि करवाएँ और चर्चा करें कि आँकड़े, कीमतें और नियम समय के साथ क्यों बदल सकते हैं।

# पहेलियों की कुंजियाँ और शिक्षक नोट

## शब्द खोज समाधान

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| सा | स | स | ई | ते | घ | इ | नी | ल | रि | द | जे | घ | छ | ई |
| के | क्से | द | प | ति | के | ट | मि | प्र | ट | सा | य | च | ऊ | नी |
| जी | ए | इ | त | म | पे | ब | प | जि | शा | मी | ने | ले | इ | सी |
| य | ट | छ | र | दे | कि | जा | सा | वा | ड | स | रे | स | ख | नि |
| फ | मो | ढ | मा | ना | सा | का | रे | दे | सि | मी | क | क | पि | ता |
| ति | रि | ज | श | भ | इ | ऊ | ने | अ | ऊ | ए | क | ने | क्श | न |
| ण | क | फ़ि | ट्रै | रि | ट | वि | श | ट | य | वि | व | वा | पा | ल |
| र | च | से | कि | य | टू | घ | प | न | व | के | की | व | सि | री |
| क | त | की | कि | सि | सा | ना | ने | लिं | पा | र्क | ते | ण | ए | ता |
| णी | सा | मी | न | नी | इ | ऋ | ले | ग | घ | ति | सु | जि | ला | ए |
| मा | जी | ले | ड | ल | ट | द | जे | घ | के | च | से | र | दे | री |
| प्र | ए | पी | उ | अ | जे | मि | घ | व | आ | च | मी | च | क्षा | ट |
| थ | फ | ग | ना | सी | का | ज | फ | नी | जी | ता | ठ | से | लि | ट |
| आ | इ | से | रा | के | री | पा | वा | सि | य | नि | पि | ने | ख | के |
| वे | ऊ | ड | नी | दे | दि | भ | आ | नि | जे | वे | वे | ष | ण | प |

## क्रॉसवर्ड समाधान




## क्रॉसवर्ड समाधान के लिए शिक्षक गाइड

### बाएँ से दाएँ

**2 बाएँ से दाएँ: साइटटूसाइट** कार्यालय नेटवर्क को आपस में जोड़ने वाली टनल (7 अक्षर)

**3 बाएँ से दाएँ: प्रशासक** वह व्यक्ति, जो संगठन के सिस्टम, खातों और अनुमतियों का प्रबंधन करता है (4 अक्षर)

**4 बाएँ से दाएँ: ट्रैफ़िक** नेटवर्क पर एक साथ आने-जाने वाला सारा डेटा (3 अक्षर)

**6 बाएँ से दाएँ: नेटवर्कसुरक्षा** नेटवर्क और उसके डेटा को अनधिकृत पहुंच और हमलों से बचाने के उपायों का समूह (7 अक्षर)

**7 बाएँ से दाएँ: टनलिंग** सुरक्षित ट्रांज़िट के लिए डेटा पैकेटों को किसी दूसरे पैकेट के भीतर लपेटना (4 अक्षर)

### ऊपर से नीचे

**1 ऊपर से नीचे: रिमोटएक्सेस** दूर बैठे कर्मचारी का कंपनी नेटवर्क और संसाधनों तक सुरक्षित रूप से पहुंचना (6 अक्षर)

**3 ऊपर से नीचे: प्रमाणीकरण** यह जांचने की प्रक्रिया कि लॉगिन करने वाला उपयोगकर्ता वास्तव में वही है जो वह होने का दावा करता है (6 अक्षर)

**5 ऊपर से नीचे: कनेक्शन** डिवाइस और सर्वर या नेटवर्क के बीच बना संपर्क, जिससे डेटा का आदान-प्रदान होता है (4 अक्षर)

# अक्षर-फेर शब्द और कूट संदेश हल कुंजी

शब्द-अनस्क्रैम्बल गतिविधि और Secret Cipher Challenge की ग्रेडिंग कुंजी।

### शब्द अनस्क्रैम्बल कुंजी

1. टूइसासाटटइ — **साइटटूसाइट**
2. कक्शनने — **कनेक्शन**
3. कफ़िट्रै — **ट्रैफ़िक**
4. सएटक्सेरिमो — **रिमोटएक्सेस**
5. कप्रसशा — **प्रशासक**
6. रवसुनेर्कक्षाट — **नेटवर्कसुरक्षा**
7. लिंटगन — **टनलिंग**
8. णीणप्ररकमा — **प्रमाणीकरण**

गुप्त कूट चुनौती कुंजी

**"ज़ीरो ट्रस्ट एंटरप्राइज़ नेटवर्क बचाता"**

# केस स्टडी के उत्तर

## A केस स्टडी 1: साझा सार्वजनिक IP का ब्लैकलिस्ट होना

शिक्षक समाधान

### ग्रेडिंग दिशानिर्देश

**छात्रों के उत्तरों में निम्नलिखित बिंदु शामिल होने चाहिए:**

- परिदृश्य विश्लेषण: एक सेल्स टीम कंज़्यूमर VPN से कॉर्पोरेट डेटाबेस तक पहुँचती है, लेकिन लॉक आउट हो जाती है क्योंकि साझा एग्ज़िट IP को धोखाधड़ी प्रणालियों ने ब्लैकलिस्ट कर दिया था।
- अनुशंसित रणनीति और समाधान: कॉर्पोरेट ट्रैफ़िक को सार्वजनिक पूल से अलग रखने के लिए स्टैटिक IP पते के साथ समर्पित बिज़नेस सर्वर तैनात करें।

## B केस स्टडी 2: कॉर्पोरेट कार्यालयों का इंटरकनेक्शन

शिक्षक समाधान

### ग्रेडिंग दिशानिर्देश

**छात्रों के उत्तरों में निम्नलिखित बिंदु शामिल होने चाहिए:**

- परिदृश्य विश्लेषण: म्यूनिख और बॉस्टन में कार्यालयों वाली एक एंटरप्राइज़ कंपनी को सार्वजनिक वेब स्पेस से ट्रैफ़िक भेजे बिना अपने स्थानीय फ़ाइल सर्वर सुरक्षित रूप से साझा करने हैं।
- अनुशंसित रणनीति और समाधान: दोनों स्थानीय ऑफ़िस नेटवर्क को इंटरनेट पर सुरक्षित रूप से जोड़ने के लिए Site-to-Site VPN टनल कॉन्फ़िगर करें।