नाम: _____ दिनांक: _____ अंक: _____

VPN क्या है वर्कशीट

नेटवर्क प्रोटोकॉल, टनलिंग और सुरक्षा नियंत्रणों में व्यावहारिक अभ्यास।

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 वर्चुअल प्राइवेट नेटवर्क (VPN) के मूल सिद्धांतों से परिचित कराता है। आप जानेंगे कि एन्क्रिप्टेड टनल आपके डेटा को कैसे सुरक्षित करती हैं, नेटवर्क प्रोटोकॉल कैसे काम करते हैं, और गोपनीयता लीक की पहचान और उन्हें कम कैसे करें।

वर्कशीट चेकपॉइंट

- [ ] **भाग 1-4: VPN अवधारणाओं और प्रोटोकॉल 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 VPN गाइड खोलें

URL: https://www.vpn.com/hi/vpn/

आपका VPN लर्निंग रोडमैप

- डेटा टनलिंग और एनकैप्सुलेशन की अवधारणा समझाएँ।
- मानक प्रोटोकॉल कॉन्फ़िगरेशन और एन्क्रिप्शन विधियों की पहचान करें।
- वर्चुअल प्राइवेट नेटवर्क में सर्वरों और IP मास्किंग की भूमिकाओं का विश्लेषण करें।
- समझें कि ISP ब्राउज़िंग को कैसे ट्रैक करते हैं और VPN इसे कैसे रोकता है।
- वर्चुअल नेटवर्क टोपोलॉजी की संचालन सीमाओं में अंतर करें।

VPN क्या है 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 केस स्टडी अनुभाग के वास्तविक परिदृश्यों पर लागू करें। अंत में अतिरिक्त गतिविधि झटपट सोचें पूरी करें।

VPN क्या है? (परिचय)

वर्चुअल प्राइवेट नेटवर्क केवल एक गोपनीयता स्विच से कहीं अधिक है। यह एक एन्क्रिप्टेड टनल है जो आपके इंटरनेट ट्रैफ़िक को रिमोट सर्वर से भेजती है। इससे आपका IP पता छिपता है, आपका ISP आपकी ऑनलाइन गतिविधियों के लॉग नहीं बना पाता, और सार्वजनिक नेटवर्क पर आपका डेटा सुरक्षित रहता है। डिजिटल सुरक्षा बनाए रखने के लिए शब्दावली को समझना ज़रूरी है।

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

चेकपॉइंट 1: बहुविकल्पीय चुनौती

1 **1. वर्चुअल प्राइवेट नेटवर्क (VPN) का मुख्य कार्य क्या है?**

- A. इंटरनेट ब्राउज़र की रेंडरिंग गति बढ़ाना
- B. डेटा पैकेट एन्क्रिप्ट करना और आपका सार्वजनिक IP छिपाना
- C. वेबसाइट कुकी डेटाबेस को लोकल रूप से संग्रहीत करने के लिए
- D. आपके भौतिक कंप्यूटर हार्डवेयर की जगह लेने के लिए

2 **2. VPN के संदर्भ में नेटवर्क टनलिंग क्या है?**

- A. डुप्लिकेट नेटवर्क लॉग फ़ाइलें हटाना
- B. स्थानीय डेटाबेस स्टोरेज फ़ाइलें इंस्टॉल करना
- C. अन्य स्थानीय कंप्यूटरों के साथ फ़ाइलें साझा करना
- D. एक नेटवर्क पैकेट को दूसरे सुरक्षित पैकेट के अंदर समाहित करना

3 **3. VPN ट्रैफ़िक की सुरक्षा के लिए कौन-सा एन्क्रिप्शन मानक व्यापक रूप से इस्तेमाल होता है?**

- A. पुराना DES एन्क्रिप्शन
- B. आधुनिक AES-256 मानक
- C. प्लेनटेक्स्ट base64 एन्कोडिंग
- D. मानक rot13 सिफ़रिंग

4 **4. VPN आपके नेटवर्क ट्रैफ़िक के किस घटक को एन्क्रिप्ट करता है?**

- A. केवल स्थानीय डिवाइस नेटवर्क के प्रिंट जॉब
- B. भौतिक ईथरनेट केबल का रूटिंग पथ
- C. नेटवर्क पैकेट का संपूर्ण डेटा पेलोड भाग
- D. केवल आपके वेब ब्राउज़र के खोज इतिहास

5 **5. नेटवर्किंग में 'एन्क्रिप्शन' शब्द का क्या अर्थ है?**

- A. सादे पाठ वाले डेटा को अपठनीय सिफ़रटेक्स्ट में बदलना
- B. पुराने संचार रिकॉर्ड मिटाना
- C. आपकी स्थानीय बैंडविड्थ गति सीमाएँ बढ़ाना
- D. डेटाबेस एक्सेस कुंजियाँ सार्वजनिक रूप से साझा करना

चेकपॉइंट 2: सही या गलत चुनौती

6 प्रश्न 6

6. VPN सार्वजनिक Wi-Fi पर स्थानीय जासूसी रोकने के लिए आपके ट्रैफ़िक को एन्क्रिप्ट करता है।

○ सही ○ गलत

7 प्रश्न 7

7. VPN आपके राउटर डिवाइस का हार्डवेयर कॉन्फ़िगरेशन भौतिक रूप से बदल देता है।

○ सही ○ गलत

8 प्रश्न 8

8. टनलिंग प्रोटोकॉल डेटा पैकेट को एन्क्रिप्टेड ट्रांसपोर्ट लेयर में लपेटते हैं।

○ सही ○ गलत

9 प्रश्न 9

9. सिमेट्रिक एन्क्रिप्शन ट्रैफ़िक को एन्क्रिप्ट और डिक्रिप्ट करने के लिए एक ही कुंजी का उपयोग करता है।

○ सही ○ गलत

10 प्रश्न 10

10. VPN का उपयोग आपके इंटरनेट कनेक्शन को ऑफ़लाइन बिजली कटौती से भौतिक रूप से अप्रभावित बना देता 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. आपका ट्रैफ़िक सुरक्षित करने के लिए VPN आपके डेटा पैकेटों को दूसरे प्रोटोकॉल में लपेटता है, जिस प्रक्रिया को _____ कहते हैं।

2. वीडियो स्ट्रीमिंग के दौरान VPN के कारण कभी-कभी _____ घट जाती है।

3. केवल किसी खास देश में उपलब्ध स्ट्रीमिंग सेवा दुनिया भर के उपयोगकर्ताओं को रोकने के लिए _____ का उपयोग करती है।

4. एन्क्रिप्शन और डेटा भेजने के पैरामीटर तय करने वाले _____ ही VPN प्रोटोकॉल कहलाते हैं।

5. आपका कंप्यूटर नेटवर्क ट्रैफ़िक की निगरानी करने और असुरक्षित कनेक्शन ब्लॉक करने के लिए स्थानीय _____ का उपयोग करता है।

6. VPN से जुड़ने पर आपके सार्वजनिक IP को छिपाने के लिए आपका डेटा किसी दूरस्थ _____ से होकर भेजा जाता है।

शब्दावली शब्द-बैंक

इंटरनेट गति | कनेक्शन नियम | जियोब्लॉक | टनलिंग | प्रोटोकॉल | फ़ायरवॉल | बैंडविड्थ | सर्वर

अपने उत्तर यहाँ लिखें:

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

चेकपॉइंट 4: नेटवर्क अवधारणा मिलान

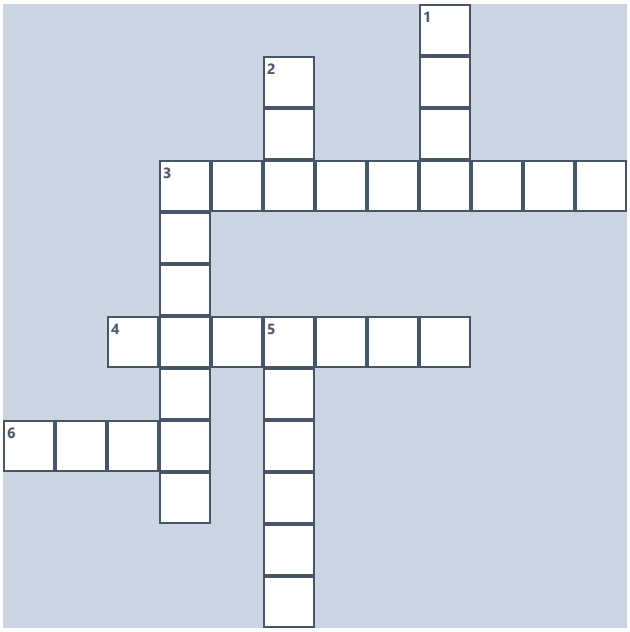
परिभाषा मिलान

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. टनलिंग**	**A**	रिमोट कंप्यूटर जो आपके ट्रैफ़िक को रूट करता है और आपका IP छिपाता है।
☐	**2. प्रोटोकॉल**	**B**	इंटरनेट सेवा प्रदाता जो आपका ट्रैफ़िक ले जाता है और असुरक्षित (बिना एन्क्रिप्शन की) गतिविधि देख सकता है।
☐	**3. बैंडविड्थ**	**C**	भौतिक स्थान के आधार पर वेब पहुँच को रोकने वाला प्रतिबंध।
☐	**4. सर्वर**	**D**	सुरक्षा प्रणाली जो अनधिकृत ट्रैफ़िक की निगरानी करती है और उसे ब्लॉक करती है।
☐	**5. जियोब्लॉक**	**E**	नियमों का समूह जो तय करता है कि नेटवर्क पर डेटा कैसे भेजा जाता है।
☐	**6. फ़ायरवॉल**	**F**	ट्रैकिंग या सार्वजनिक निगरानी से मुक्त होने की स्थिति।
☐	**7. गोपनीयता**	**G**	किसी कनेक्शन पर डेटा ट्रांसफ़र की अधिकतम दर।
☐	**8. ISP**	**H**	सुरक्षित ट्रांज़िट के लिए डेटा पैकेट को दूसरे पैकेट के भीतर लपेटना।

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

3. उपकरण को वेब से जोड़ने वाली सेवा। (9)

4. एन्क्रिप्शन और डेटा भेजने के पैरामीटर तय करने वाले नियम। (7)

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

ऊपर से नीचे

1. भौतिक स्थान के आधार पर वेब पहुँच रोकने वाली पाबंदी (4)

2. दूरस्थ कंप्यूटर, जो आपका ट्रैफ़िक रूट करता है और आपका IP छिपाता है (3)

3. आपके कनेक्शन पर डेटा के आने-जाने की रफ़्तार। (7)

5. वीपीएन सर्वर द्वारा दिया गया पता, जो असली पहचान छिपा देता है। (6)

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

3 बाएँ से दाएँ: उपकरण को वेब से जोड़ने वाली सेवा। (9 अक्षर):

4 बाएँ से दाएँ: एन्क्रिप्शन और डेटा भेजने के पैरामीटर तय करने वाले नियम। (7 अक्षर):

6 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: भौतिक स्थान के आधार पर वेब पहुँच रोकने वाली पाबंदी (4 अक्षर):

2 ऊपर से नीचे: दूरस्थ कंप्यूटर, जो आपका ट्रैफ़िक रूट करता है और आपका IP छिपाता है (3 अक्षर):

3 ऊपर से नीचे: आपके कनेक्शन पर डेटा के आने-जाने की रफ़्तार। (7 अक्षर):

5 ऊपर से नीचे: वीपीएन सर्वर द्वारा दिया गया पता, जो असली पहचान छिपा देता है। (6 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।

जा	सा	वा	ड	रे	स	ख	फ़ा	नि	फ	ढ	मा	ना	का	रे
दे	सि	मी	क	पि	ता	ति	य	न	ज	श	भ	ऊ	अ	ऊ
ए	रि	क	वि	श	य	वि	र	व	क	वा	पा	ल	च	से
कि	य	ब्लॉ	घ	प	के	की	वॉ	व	सि	ली	री	त	की	कि
सि	ना	यो	ने	पा	इं	ते	ल	ण	ए	ट	आ	ता	सा	मी
म	न	जि	नी	ऋ	ट	ले	इं	घ	ति	जि	न	ई	ला	ए
य	जी	ले	ड	ल	र	द	जे	ट	घ	के	च	लिं	पी	से
नि	दे	री	ए	पी	ने	उ	अ	जे	र	मि	घ	व	ग	आ
न	च	मी	च	ट	ट	थ	फ	ग	ना	ने	सी	का	ज	फ
क्श	नी	जी	ता	ठ	क	से	लि	ट	आ	इ	ट	से	रा	के
ने	री	पा	वा	सि	ने	य	नि	पि	ने	ख	के	ग	वे	ऊ
क	ड	नी	दे	दि	क्श	भ	आ	नि	र	जे	वे	वे	ति	ष
ण	प	कि	से	य	न	ह	ह	र्व	ते	रा	द	सा	सी	थ
जे	इ	मे	ला	ढ	पे	ऋ	स	वे	नी	वे	उ	थ	ह	जे
त	य	मी	रे	मि	दि	ए	ह	जे	जा	ढ	वी	रा	दा	पी

शब्दावली शब्द-सूची

टनलिंग · इंटरनेटगति · जियोब्लॉक · कनेक्शननियम · फ़ायरवॉल · सर्वर · नकलीआईपी · इंटरनेटकनेक्शन

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. टनलिंग**
- **B. इंटरनेटगति**
- **C. जियोब्लॉक**
- **D. कनेक्शननियम**
- **E. फ़ायरवॉल**
- **F. सर्वर**
- **G. नकलीआईपी**
- **H. इंटरनेटकनेक्शन**

परिभाषाएँ और मिलान फ़ील्ड

1. आपके कनेक्शन पर डेटा के आने-जाने की रफ़्तार।
2. सुरक्षा प्रणाली, जो अनधिकृत ट्रैफ़िक की निगरानी करती है और उसे ब्लॉक करती है।
3. दूरस्थ कंप्यूटर, जो आपका ट्रैफ़िक रूट करता है और आपका IP छिपाता है।
4. वीपीएन सर्वर द्वारा दिया गया पता, जो असली पहचान छिपा देता है।
5. उपकरण को वेब से जोड़ने वाली सेवा।
6. सुरक्षित ट्रांज़िट के लिए डेटा पैकेटों को किसी दूसरे पैकेट के भीतर लपेटना।
7. एन्क्रिप्शन और डेटा भेजने के पैरामीटर तय करने वाले नियम।
8. भौतिक स्थान के आधार पर वेब पहुँच रोकने वाली पाबंदी।

चेकपॉइंट 7: उलझे शब्दों की चुनौती

नीचे के अक्षरों को सुलझाकर VPN की प्रमुख अवधारणाएँ और शब्द पता करें। अपने उत्तर भरे जा सकने वाले इनपुट बॉक्स में लिखें।

1. लिं ट ग न
2. जि ब्लॉ क यो
3. र फ़ा ल वॉ य
4. पी आ ली ई न क
5. ट ति ने र इं ग ट
6. य क्श नि क न म ने
7. र र्व स
8. न ट क्श इं ने ट क ने र

अतिरिक्त गतिविधि: झटपट सोचें

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

1	ऐसी चीज़ें जो IP एड्रेस उजागर कर सकता है			
2	VPN के बारे में मिथक			
3	इंटरनेट पर यात्रा करने वाली चीज़ें			
4	अच्छे VPN प्रदाता के वादे			
5	ऐसे राज़ जिन्हें आप एन्क्रिप्ट करेंगे			
6	ऐसी चीज़ें जिनसे VPN आपको नहीं बचा सकता			
7	नकली Wi-Fi नेटवर्क पहचानने के तरीके			
8	गोपनीयता से जुड़े शब्द			
9	ऐसे डिवाइस जो VPN इस्तेमाल कर सकते हैं			
10	'Connect' दबाने पर होने वाली चीज़ें			
11	ऐसी जगहें जहाँ आप VPN इस्तेमाल करेंगे			
12	यात्रा के दौरान VPN इस्तेमाल करने के कारण			
13	असल ज़िंदगी की ऐसी चीज़ें जो टनल जैसी दिखती हैं			
14	इस वर्कशीट के वे शब्द जिन्हें आप याद रखना चाहते हैं			
15	बच्चे को VPN समझाने के लिए शब्द			

चेकपॉइंट 8: VPN केस स्टडी

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

सारा (कॉफ़ी शॉप की छात्रा)

👱 "नमस्ते! मैं Coffee & Bytes में बैठा हूँ। यहाँ 'Free_Wi-Fi_No_Password' नाम का एक असुरक्षित सार्वजनिक नेटवर्क है। मैं अपने स्कूल के ईमेल में लॉग इन करना और अपना असाइनमेंट अपलोड करना चाहता हूँ, लेकिन मुझे हैकरों की चिंता है। VPN के बिना इस नेटवर्क का उपयोग करने के क्या जोखिम हैं, और VPN मेरे डेटा को कैसे सुरक्षित करता है?"

Alex (यात्री छात्र)

👱 "अरे नहीं! मैं एक प्रोजेक्ट के लिए विदेश यात्रा पर हूँ और अपने गृह देश के एक सर्वर पर होस्ट की गई जीव विज्ञान डॉक्यूमेंट्री देखने की कोशिश कर रहा हूँ। लेकिन साइट पर लिखा आ रहा है 'यह वीडियो आपकी वर्तमान लोकेशन में उपलब्ध नहीं है।' मुझे ब्लॉक क्यों किया जा रहा है, और VPN इसे देखने में कैसे मदद कर सकता है?"

चेकपॉइंट 9: कूट संदेश को डिकोड करें

VPN आपके ट्रैफ़िक को सुरक्षित करने के लिए उसे एन्क्रिप्ट करता है। नीचे दी गई अक्षर-से-संख्या कुंजी का उपयोग करके साइबर सुरक्षा 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

44	49	39	13	61	43	47	28		23	32	40		44	52		1	33	32	48

15	54	33	32	48	38	28	46		35	18	46	8	58

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 के उपयोग के बारे में संभावित ग्राहकों के सबसे आम सवाल और जवाब देखें।

Q1: VPN क्या है और यह कैसे काम करता है?

वर्चुअल प्राइवेट नेटवर्क (VPN) आपके इंटरनेट कनेक्शन को एन्क्रिप्ट करता है और आपके ट्रैफ़िक को एक सुरक्षित रिमोट सर्वर से भेजता है। इससे आपका सार्वजनिक IP पता छिप जाता है और VPN टनल से गुज़रने वाले ट्रैफ़िक के बारे में स्थानीय नेटवर्क पर नज़र रखने वाले और आपका ISP जो देख सकते हैं, वह सीमित हो जाता है।

Q2: मुझे VPN का उपयोग क्यों करना चाहिए?

VPN आपकी डिजिटल गोपनीयता की रक्षा करता है, सार्वजनिक Wi-Fi नेटवर्क (जैसे कैफ़े या हवाई अड्डे) पर आपके कनेक्शन को सुरक्षित करता है, जब ISP एन्क्रिप्टेड ट्रैफ़िक का प्रकार पहचान नहीं पाता तब गतिविधि-आधारित थ्रॉटलिंग को घटा सकता है, वैश्विक सामग्री तक पहुँचने के लिए भौगोलिक प्रतिबंधों को बायपास करता है, और दूरस्थ कार्य के संसाधनों को सुरक्षित करने में मदद करता है।

Q3: क्या VPN मुझे ऑनलाइन पूरी तरह गुमनाम बना देता है?

नहीं। VPN आपका IP पता छिपाता है और ट्रैफ़िक एन्क्रिप्ट करता है, फिर भी आपको ब्राउज़र कुकी, सक्रिय खातों (जैसे Google या Facebook), ब्राउज़र फ़िंगरप्रिंटिंग, या VPN प्रदाता द्वारा आपका डेटा लॉग करने से ट्रैक किया जा सकता है।

Q4: क्या VPN मेरी इंटरनेट स्पीड धीमी कर देगा?

हाँ, थोड़ी। एन्क्रिप्शन प्रक्रिया और VPN सर्वर की भौतिक दूरी लेटेंसी और ओवरहेड बढ़ाती है। असर प्रोवाइडर, प्रोटोकॉल, सर्वर की दूरी, डिवाइस और नेटवर्क की स्थिति के अनुसार बदलता है।

Q5: क्या VPN का उपयोग क़ानूनी है?

कई देशों में VPN का उपयोग कानूनी है, लेकिन कुछ क्षेत्राधिकार VPN सेवाओं को प्रतिबंधित, विनियमित या ब्लॉक करते हैं। उपयोग से पहले उपयोगकर्ताओं को वर्तमान स्थानीय कानून जाँच लेने चाहिए। अधिक जानकारी के लिए VPN.com पर वैधता गाइड देखें।

चेकपॉइंट 10: बुनियादी VPN FAQ (भाग B)

वर्चुअल प्राइवेट नेटवर्क के उपयोग के बारे में संभावित ग्राहकों के सबसे आम सवाल और जवाब देखें।

Q6: क्या मैं मुफ़्त VPN उपयोग कर सकता हूँ?

मुफ़्त VPN विज्ञापन, सीमित सुविधाओं, उपयोग विश्लेषण, डेटा सीमा या कमाई के अन्य मॉडलों पर निर्भर हो सकते हैं। उपयोग से पहले उपयोगकर्ताओं को प्रदाता की गोपनीयता नीति, स्वामित्व, ऑडिट और बिज़नेस मॉडल की समीक्षा करनी चाहिए।

Q7: "नो-लॉग्स" नीति क्या है?

नो-लॉग्स नीति बताती है कि प्रदाता के अनुसार वह कौन-सी गतिविधि और कनेक्शन डेटा नहीं रखता। सटीक दायरा अलग-अलग होता है, इसलिए पाठकों को नीति और स्वतंत्र ऑडिट के निष्कर्ष देखने चाहिए।

Q8: मैं सबसे अच्छा VPN कैसे चुनूँ?

ऑडिट की गई नो-लॉग्स नीतियाँ, मज़बूत प्रोटोकॉल (WireGuard, OpenVPN), सुरक्षित सर्वर स्थान, तेज़ गति, केवल-RAM सर्वर, किल स्विच सुविधा और खुफ़िया-साझाकरण गठबंधनों (जैसे 5/9/14 Eyes) से बाहर का क्षेत्राधिकार देखें।

Q9: क्या मैं अपने फ़ोन और स्मार्ट TV पर VPN उपयोग कर सकता हूँ?

हाँ। आधुनिक VPN प्रोवाइडर iOS, Android, macOS, Windows, Linux और स्मार्ट टीवी के लिए समर्पित ऐप्स, साथ ही आपके घर के नेटवर्क के सभी डिवाइस की सुरक्षा के लिए राउटर सेटअप देते हैं।

Q10: Kill Switch क्या है?

Kill Switch एक सुरक्षा सुविधा है जो VPN कनेक्शन टूटने पर आपके उपकरण को इंटरनेट से अपने-आप डिस्कनेक्ट कर देती है। इससे आपका बिना एन्क्रिप्शन वाला डेटा या असली IP पता लीक होने से बचता है।

चेकपॉइंट 10: उन्नत VPN FAQ (भाग C)

वर्चुअल प्राइवेट नेटवर्क और सुरक्षित टनलिंग प्रोटोकॉल के तकनीकी और संरचनात्मक पहलुओं को जानें।

Q1: WireGuard, OpenVPN और IKEv2 में क्या अंतर है?

WireGuard एक आधुनिक, हल्का प्रोटोकॉल है (केवल ~4,000 कोड लाइनें) जो तेज़ गति और जल्दी कनेक्शन समय देता है। OpenVPN एक अत्यंत सुरक्षित, कसौटी पर परखा हुआ ओपन-सोर्स प्रोटोकॉल है। IKEv2 नेटवर्क बदलते समय जल्दी फिर से कनेक्ट होने की क्षमता के कारण मोबाइल डिवाइस के लिए उत्कृष्ट है। [4]

Q2: डबल VPN या Multi-Hop रूटिंग क्या है?

मल्टी-हॉप आपके ट्रैफ़िक को क्रम में दो या अधिक VPN सर्वरों से रूट करता है। इससे एन्क्रिप्शन की दूसरी परत जुड़ती है और अगर एक सर्वर से समझौता हो जाए, तो आपके असली IP पते को दूसरे हॉप से छिपाए रखने में मदद मिलती है।

Q3: WebRTC लीकिंग क्या है और VPN इसे कैसे रोकता है?

WebRTC एक ब्राउज़र प्रोटोकॉल है जो VPN सक्रिय होने पर भी आपके असली लोकल और सार्वजनिक IP पते उजागर कर सकता है। प्रीमियम VPN अपने डेस्कटॉप/मोबाइल ऐप और ब्राउज़र एक्सटेंशन में WebRTC अनुरोधों को ब्लॉक या स्पूफ़ करते हैं।

Q4: RAM-only सर्वर क्या हैं और वे क्यों मायने रखते हैं?

पारंपरिक सर्वर डेटा हार्ड ड्राइव पर लिखते हैं, जिन्हें ज़ब्त या समझौता किया जा सकता है। केवल-RAM (बिना डिस्क वाले) सर्वर पूरी तरह वोलेटाइल मेमोरी (RAM) में चलते हैं। सर्वर के रीबूट या बंद होने पर मेमोरी में रखा डेटा मिट जाता है।

Q5: ऑब्फ़स्केशन VPN ब्लॉक को कैसे बायपास करता है?

ऑब्फ़स्केशन (या "Stealth VPN") VPN ट्रैफ़िक को ऐसा रूप देता है कि वह सामान्य HTTPS ट्रैफ़िक (पोर्ट 443) जैसा दिखे। इससे सरकारों या स्कूल/ऑफ़िस नेटवर्क द्वारा VPN रोकने के लिए इस्तेमाल की जाने वाली डीप पैकेट इंस्पेक्शन (DPI) को पार करने में मदद मिल सकती है।

चेकपॉइंट 10: उन्नत VPN FAQ (भाग D)

वर्चुअल प्राइवेट नेटवर्क और सुरक्षित टनलिंग प्रोटोकॉल के तकनीकी और संरचनात्मक पहलुओं को जानें।

Q6: स्प्लिट टनलिंग क्या है और इसका उपयोग कब करना चाहिए?

स्प्लिट टनलिंग आपको चुनने देती है कि कौन से ऐप एन्क्रिप्टेड VPN टनल से जाएँ और कौन सीधे इंटरनेट से जुड़ें। संवेदनशील बैंकिंग ऐप को VPN से भेजने और स्थानीय गेम को सीधे जोड़ने के लिए इसका उपयोग करें, जिससे VPN से जुड़ी लेटेंसी से बचा जा सके।

Q7: फ़ॉरवर्ड सीक्रेसी (परफ़ेक्ट फ़ॉरवर्ड सीक्रेसी) कैसे काम करती है?

PFS यह सुनिश्चित करता है कि हर सत्र के लिए एक अनूठी, अस्थायी एन्क्रिप्शन कुंजी बने। भविष्य में प्राइवेट कुंजी से छेड़छाड़ हो भी जाए, तो उससे पिछले या भविष्य के सत्र डिक्रिप्ट नहीं किए जा सकते क्योंकि उनमें स्वतंत्र कुंजियाँ इस्तेमाल हुई थीं।

Q8: 5/9/14 Eyes गठबंधन क्या हैं और मुझे इनकी परवाह क्यों करनी चाहिए?

क्षेत्राधिकार उस कानूनी प्रक्रिया को प्रभावित कर सकता है जिसका सामना कोई प्रदाता कर सकता है, लेकिन व्यावहारिक गोपनीयता जोखिम इस पर भी निर्भर करता है कि प्रदाता कौन-सा डेटा रखता है, उसका तकनीकी ढाँचा, स्वामित्व, पारदर्शिता रिपोर्टिंग और ऑडिट का इतिहास क्या है।

Q9: DNS Leak सुरक्षा क्या है?

DNS लीक सुरक्षा आपके डिवाइस को वेबसाइट लुकअप क्वेरी (DNS क्वेरी) अपने ISP के सर्वरों के बजाय VPN के निजी, एन्क्रिप्टेड DNS सर्वरों से भेजने के लिए बाध्य करती है। इससे आपका ISP यह ट्रैक नहीं कर पाता कि आप कौन-सी साइटें देखते हैं।

Q10: क्या VPN ISP इंटरनेट थ्रॉटलिंग को बायपास कर सकता है?

कभी-कभी। जब ISP चुनिंदा पहचान योग्य गतिविधियों की स्पीड घटाता है, तब VPN मदद कर सकता है, लेकिन वह भीड़, डेटा सीमा, खाता-स्तर की स्पीड सीमा या खराब नेटवर्क गुणवत्ता को दूर नहीं करेगा।

भाग 11: 10 रोचक VPN तथ्य और वास्तविक दुनिया की अंतर्दृष्टियाँ

VPN के इतिहास, बाज़ार और तकनीक से जुड़े इन बेहद उपयोगी, वास्तविक तथ्यों और अंतर्दृष्टियों को देखें।

1. पहला VPN प्रोटोकॉल

PPTP (Point-to-Point Tunneling Protocol) को Microsoft समेत एक वेंडर समूह ने विकसित किया था और रिमोट-एक्सेस VPN को सपोर्ट करने के लिए इसे जुलाई 1999 में RFC 2637 के रूप में प्रकाशित किया गया। [6]

2. बाज़ार मूल्यांकन

दूरस्थ कार्य की बढ़ती ज़रूरतों और उद्यमों की सुरक्षा माँग के कारण वैश्विक VPN बाज़ार में तेज़ वृद्धि हुई है।

3. WireGuard क्रांति

WireGuard में दक्षता के लिए डिज़ाइन किया गया अत्यंत सुव्यवस्थित कोडबेस है, जिससे पारंपरिक प्रोटोकॉल की तुलना में सुरक्षा कमज़ोरियों के लिए उसका ऑडिट करना आसान होता है। [4]

4. सख़्त ऑडिटिंग मानक

शीर्ष VPN प्रदाता स्वतंत्र कोड समीक्षा करने और यह सत्यापित करने के लिए बाहरी ऑडिटर (जैसे Cure53 या PwC) रखते हैं कि वे उपयोगकर्ता की कोई गतिविधि लॉग नहीं करते।

5. 5-Eyes गठबंधन की उत्पत्ति

Five Eyes गठबंधन अमेरिका और ब्रिटेन के बीच 1946 के UKUSA सिग्नल्स-इंटेलिजेंस समझौते से विकसित हुआ, जिसमें बाद में कनाडा, ऑस्ट्रेलिया और न्यूज़ीलैंड शामिल हुए।

6. डीप पैकेट इंस्पेक्शन

डीप पैकेट इंस्पेक्शन (DPI) केवल हेडर ही नहीं, पैकेट की सामग्री और ट्रैफ़िक पैटर्न की भी जाँच करता है, और कुछ फ़ायरवॉल इसका उपयोग आम VPN प्रोटोकॉल को पहचानने और ब्लॉक करने के लिए करते हैं।

7. कॉर्पोरेट उपयोग

दुनिया भर में बड़ी संख्या में एंटरप्राइज़ कर्मचारी आंतरिक डेटाबेस में लॉग इन करने के लिए सुरक्षित VPN का उपयोग करते हैं, जिससे यह एक प्रमुख सुरक्षा मानक बन गया है।

8. विकेंद्रीकृत VPN

विकेंद्रीकृत VPN (dVPN) ट्रैफ़िक को पीयर-संचालित नोड के नेटवर्क में बाँटते हैं, जिससे किसी एक केंद्रीकृत प्रदाता पर निर्भरता घटती है।

9. TOR बनाम VPN गुमनामी

VPN ट्रैफ़िक को एक ही प्रदाता के ज़रिए टनल करता है, जबकि Tor (The Onion Router) ट्रैफ़िक को तीन स्वयंसेवी रिले (गार्ड, मिडिल और एग्ज़िट) से भेजता है, ताकि कोई एक रिले दोनों सिरों को न जान सके।

10. डेटा उल्लंघनों की लागत

VPN के साथ ज़ीरो-ट्रस्ट सुरक्षित एक्सेस मॉडल अपनाने से संगठनों को बौद्धिक संपदा की रक्षा करने और डेटा उल्लंघनों के वित्तीय प्रभाव को घटाने में मदद मिलती है।

तकनीकी संदर्भ और स्रोत

इस वर्कशीट में उपयोग किए गए उद्धृत प्रकाशन, क्रिप्टोग्राफ़िक विनिर्देश और आधिकारिक दस्तावेज़ मानक।

शैक्षणिक और उद्योग संदर्भ

[1] NIST. (2020). SP 800-77 Rev. 1: Guide to IPsec VPNs.
https://csrc.nist.gov/pubs/sp/800/77/r1/final

[2] WireGuard. (n.d.). WireGuard: fast, modern, secure VPN tunnel.
https://www.wireguard.com/

[3] WireGuard. (n.d.). Protocol & Cryptography.
https://www.wireguard.com/protocol/

[4] Donenfeld, J. A. (2017). WireGuard: Next Generation Kernel Network Tunnel. NDSS Symposium.
https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/wireguard-next-generation-kernel-network-tunnel/

[5] OpenVPN. (n.d.). OpenVPN 2.6 Manual.
https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/

[6] IETF. (1999). RFC 2637: Point-to-Point Tunneling Protocol (PPTP).
https://datatracker.ietf.org/doc/html/rfc2637

उत्तर कुंजी: VPN क्या है वर्कशीट

1 **मुख्य कार्य** प्रोटोकॉल **सही उत्तर: B**

शिक्षण नोट

VPN का मुख्य काम एक एन्क्रिप्टेड टनल बनाना है जो पैकेट पेलोड डेटा की रक्षा करती है और उपयोगकर्ता का सार्वजनिक IP पता छिपाती है। संदर्भ: IETF Tunnel RFC।

2 **नेटवर्क टनलिंग** लेटेंसी **सही उत्तर: D**

शिक्षण नोट

टनलिंग प्रोटोकॉल मूल डेटा पैकेट को बाहरी वाहक पैकेट के अंदर एनकैप्सुलेट करते हैं, ताकि वे सार्वजनिक नेटवर्क से सुरक्षित गुज़र सकें। उद्धरण: IETF Tunnel RFC।

3 **प्रश्न 3** **सही उत्तर: B**

शिक्षण नोट

VPN ट्रैफ़िक की सुरक्षा के लिए कौन-सा एन्क्रिप्शन मानक व्यापक रूप से इस्तेमाल होता है? → आधुनिक AES-256 मानक

4 **एन्क्रिप्टेड घटक** रूटिंग नियंत्रण **सही उत्तर: C**

शिक्षण नोट

VPN IP डेटा पैकेट के पूरे पेलोड खंड को एन्क्रिप्ट करता है, जिससे ट्रांसमिशन की सामग्री गोपनीय रहती है। संदर्भ: IETF Tunnel RFC।

5 **प्रश्न 5** **सही उत्तर: A**

शिक्षण नोट

एन्क्रिप्शन एक एल्गोरिदम और कुंजी का उपयोग करके प्लेनटेक्स्ट को अपठनीय सिफ़रटेक्स्ट में बदलता है।

उत्तर कुंजी: चेकपॉइंट 2 – सही या गलत

6 **छिपकर सुनने पर रोक** IP मास्किंग **सही उत्तर: सही**

शिक्षण नोट

एन्क्रिप्टेड टनल यह सुनिश्चित करती हैं कि स्थानीय Wi-Fi नेटवर्क पर डेटा रोकने वालों को पैकेट पेलोड पढ़ने योग्य न मिलें। उद्धरण: Deloitte Advisory।

7 **हार्डवेयर परिवर्तन** गति **सही उत्तर: गलत**

शिक्षण नोट

VPN सॉफ़्टवेयर-आधारित नेटवर्क टनल हैं और आपके गेटवे राउटर हार्डवेयर को भौतिक रूप से नहीं बदलते। उद्धरण: Cure53 Audit।

8 **टनलिंग पैकेट** स्निफ़िंग का जोखिम **सही उत्तर: सही**

शिक्षण नोट

टनलिंग मूल नेटवर्क पैकेट को पारगमन के लिए ट्रांसपोर्ट हेडर के भीतर लपेटकर काम करती है। उद्धरण: IETF Tunnel RFC।

9 **सिमेट्रिक कुंजियाँ** फ़ायरवॉल **सही उत्तर: सही**

शिक्षण नोट

सिमेट्रिक क्रिप्टोग्राफ़ी नेटवर्क स्ट्रीम को एन्क्रिप्ट और डिक्रिप्ट करने, दोनों के लिए एक साझा कुंजी का उपयोग करती है। उद्धरण: WireGuard Project।

10 **पावर इम्यूनिटी** नो-लॉग्स **सही उत्तर: गलत**

शिक्षण नोट

VPN केवल सक्रिय कनेक्शन सिग्नल को एन्क्रिप्ट करता है; वह स्थानीय बिजली कटौती से होने वाले सेवा-व्यवधान को नहीं रोक सकता। संदर्भ: EDRi Retention Guidelines।

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

H 1. टनलिंग	E 2. प्रोटोकॉल	G 3. बैंडविड्थ	A 4. सर्वर
C 5. जियोब्लॉक	D 6. फ़ायरवॉल	F 7. गोपनीयता	B 8. ISP

चेकपॉइंट 3: उत्तर – प्रमुख शब्द

1 टनलिंग	2 इंटरनेट गति	3 जियोब्लॉक	4 कनेक्शन नियम
5 फ़ायरवॉल	6 सर्वर		

चेकपॉइंट 6, वैकल्पिक: उत्तर – शब्द मिलान

1 B – इंटरनेटगति	2 E – फ़ायरवॉल	3 F – सर्वर	4 G – नकलीआईपी
5 H – इंटरनेटकनेक्शन	6 A – टनलिंग	7 D – कनेक्शननियम	8 C – जियोब्लॉक

शिक्षकों के लिए चर्चा नोट

प्रमुख शब्द:
जाँचें कि क्या विद्यार्थी टनलिंग, प्रोटोकॉल और बैंडविड्थ 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।

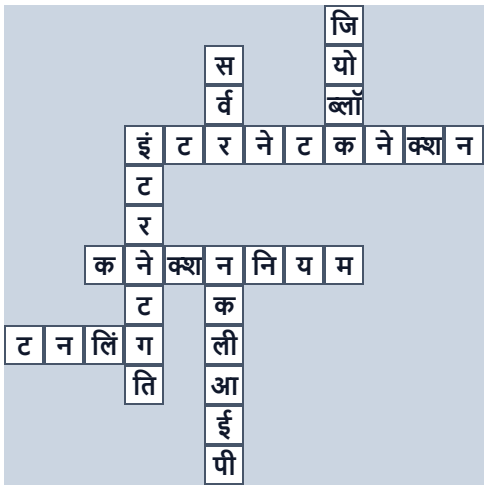
स्रोतों का मूल्यांकन:
विद्यार्थियों से वर्कशीट के स्रोतों में कम से कम एक कथन की पुष्टि करवाएँ और चर्चा करें कि आँकड़े, कीमतें और नियम समय के साथ क्यों बदल सकते हैं।

पहेलियों की कुंजियाँ और शिक्षक नोट

शब्द खोज समाधान

जा	सा	वा	ड	रे	स	ख	फ़ा	नि	फ	ढ	मा	ना	का	रे
दे	सि	मी	क	पि	ता	ति	य	न	ज	श	भ	ऊ	अ	ऊ
ए	रि	क	वि	श	य	वि	र	व	क	वा	पा	ल	च	से
कि	य	ब्लॉ	घ	प	के	की	वॉ	व	सि	ली	री	त	की	कि
सि	ना	यो	ने	पा	इं	ते	ल	ण	ए	ट	आ	ता	सा	मी
म	न	जि	नी	ऋ	ट	ले	इं	घ	ति	जि	न	ई	ला	ए
य	जी	ले	ड	ल	र	द	जे	ट	घ	के	च	लिं	पी	से
नि	दे	री	ए	पी	ने	उ	अ	जे	र	मि	घ	व	ग	आ
न	च	मी	च	ट	ट	थ	फ	ग	ना	ने	सी	का	ज	फ
क्श	नी	जी	ता	ठ	क	से	लि	ट	आ	इ	ट	से	रा	के
ने	री	पा	वा	सि	ने	य	नि	पि	ने	ख	के	ग	वे	ऊ
क	ड	नी	दे	दि	क्श	भ	आ	नि	र	जे	वे	वे	ति	ष
ण	प	कि	से	य	न	ह	ह	र्व	ते	रा	द	सा	सी	थ
जे	इ	मे	ला	ढ	पे	ऋ	स	वे	नी	वे	उ	थ	ह	जे
त	य	मी	रे	मि	दि	ए	ह	जे	जा	ढ	वी	रा	दा	पी

क्रॉसवर्ड समाधान



क्रॉसवर्ड समाधान के लिए शिक्षक गाइड

बाएँ से दाएँ

3 बाएँ से दाएँ: इंटरनेटकनेक्शन उपकरण को वेब से जोड़ने वाली सेवा। (9 अक्षर)

4 बाएँ से दाएँ: कनेक्शननियम एन्क्रिप्शन और डेटा भेजने के पैरामीटर तय करने वाले नियम। (7 अक्षर)

6 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: जियोब्लॉक भौतिक स्थान के आधार पर वेब पहुँच रोकने वाली पाबंदी (4 अक्षर)

2 ऊपर से नीचे: सर्वर दूरस्थ कंप्यूटर, जो आपका ट्रैफ़िक रूट करता है और आपका IP छिपाता है (3 अक्षर)

3 ऊपर से नीचे: इंटरनेटगति आपके कनेक्शन पर डेटा के आने-जाने की रफ़्तार। (7 अक्षर)

5 ऊपर से नीचे: नकलीआईपी वीपीएन सर्वर द्वारा दिया गया पता, जो असली पहचान छिपा देता है। (6 अक्षर)

अक्षर-फेर शब्द और कूट संदेश हल कुंजी

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

शब्द अनस्क्रैम्बल कुंजी

1. लिंटगन — **टनलिंग**
2. जिब्लॉकयो — **जियोब्लॉक**
3. रफ़ालवॉय — **फ़ायरवॉल**
4. पीआलीईनक — **नकलीआईपी**
5. टतिनेरइंगट — **इंटरनेटगति**
6. यक्शनिकनमने — **कनेक्शननियम**
7. रर्वस — **सर्वर**
8. नटक्शइंनेटकनेर — **इंटरनेटकनेक्शन**

गुप्त कूट चुनौती कुंजी

"सुरक्षित टनल से अपनी गोपनीयता बचाएँ"

केस स्टडी के उत्तर

A परिदृश्य A: सार्वजनिक नेटवर्क की सुरक्षा

स्निफ़िंग और एन्क्रिप्शन सारा की दुविधा

ग्रेडिंग दिशानिर्देश

छात्रों के उत्तरों में निम्नलिखित बिंदु शामिल होने चाहिए:

- जोखिम: पैकेट स्निफ़िंग, डेटा इंटरसेप्शन और मैन-इन-द-मिडिल हमले। उसी कॉफ़ी शॉप नेटवर्क पर मौजूद कोई व्यक्ति उसके लॉगिन विवरण या होमवर्क फ़ाइल को कैप्चर कर सकता है।
- VPN सुरक्षा: नेटवर्क पैकेट पेलोड को एन्क्रिप्ट करती है, जिससे VPN के सही कॉन्फ़िगर होने पर इंटरसेप्ट किया गया टनल ट्रैफ़िक निष्क्रिय स्थानीय-नेटवर्क जासूसों के लिए अपठनीय हो जाता है।

B परिदृश्य B: ब्लॉक किए गए संसाधनों तक पहुँचना

जियो-ब्लॉकिंग और IP Alex की दुविधा

ग्रेडिंग दिशानिर्देश

छात्रों के उत्तरों में निम्नलिखित बिंदु शामिल होने चाहिए:

- ब्लॉक होने का कारण: स्ट्रीमिंग होस्ट जियो-ब्लॉकिंग का उपयोग करता है, जो यात्री के लोकल IP पते को उसके भौतिक देश से जोड़ता है और क्षेत्रीय लाइसेंसिंग के आधार पर उसे ब्लॉक कर देता है।
- VPN कैसे मदद करता है: ट्रैफ़िक को उसके गृह देश के सर्वर से गुज़ारकर उसकी असली लोकेशन छिपाना। साइट को गृह देश का IP दिखता है, जिससे एक्सेस मिल जाता है।