नाम: _____ दिनांक: _____ अंक: _____

VPN कैसे सेट अप करें वर्कशीट

Windows, macOS, Android, iOS, Linux और राउटरों पर VPN कॉन्फ़िगर करना

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

- व्यावसायिक VPN ऐप की तुलना नेटिव क्लाइंट सेट करने से करें।
- पूरे घर की सुरक्षा के लिए राउटर पर VPN कनेक्शन कॉन्फ़िगर करें।
- OVPN या WireGuard कुंजियों जैसी कॉन्फ़िगरेशन फ़ाइलें सेट और प्रबंधित करें।
- टनल ट्रैफ़िक के लिए राउटर के विशिष्ट पोर्ट खोलें और सुरक्षित करें।
- DNS लीक जाँच और कनेक्शन टेस्ट के ज़रिए क्लाइंट सेटअप सत्यापित करें।

कॉन्फ़िगरेशन वर्कशीट के 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 VPN क्लाइंट सेट अप करने और उनका परीक्षण करने पर लागू करें। अंत में अतिरिक्त गतिविधि झटपट सोचें पूरी करें।

VPN कॉन्फ़िगरेशन (परिचय)

VPN को मैन्युअल रूप से सेट करने से आपको अपनी एन्क्रिप्शन कुंजियों और नेटवर्क रूटिंग पर पूरा नियंत्रण मिलता है। चाहे आप अपने मोबाइल डिवाइस पर नेटिव क्लाइंट कॉन्फ़िगर करें या सीधे राउटर पर VPN टनल इंस्टॉल करें, DNS लीक रोकने और सारे नेटवर्क ट्रैफ़िक को सुरक्षित करने के लिए सही कॉन्फ़िगरेशन ज़रूरी है।

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

चेकपॉइंट 1: बहुविकल्पीय चुनौती

1 **1. मोबाइल डिवाइस पर VPN सेट अप करने का सबसे आसान तरीका क्या है?**

- A. ऐप स्टोर से आधिकारिक VPN ऐप डाउनलोड करना
- B. ऑपरेटिंग सिस्टम की कर्नेल फ़ाइलों को मैन्युअल रूप से एडिट करना
- C. डिवाइस हार्डवेयर पर कस्टम फ़र्मवेयर फ़्लैश करना
- D. फ़ोन को USB से डेस्कटॉप कंप्यूटर से जोड़ना

2 **2. VPN को सीधे अपने राउटर पर इंस्टॉल करने का एक लाभ क्या है?**

- A. यह सभी स्थानीय उपकरणों की कनेक्शन गति बढ़ाता है
- B. यह जुड़े हुए सभी नेटवर्क डिवाइस को अपने आप सुरक्षित कर देता है
- C. यह स्थानीय ISP सदस्यता शुल्क की ज़रूरत को बायपास करता है
- D. यह हार्डवेयर राउटरों की ज़रूरत को पूरी तरह खत्म कर देता है

3 **3. 'नेटिव' VPN कॉन्फ़िगरेशन से क्या तात्पर्य है?**

- A. OS की मूल अंतर्निहित सेटिंग से कनेक्शन सेट करना
- B. VPN का उपयोग केवल अपने गृह नगर में करना
- C. केवल स्थानीय देश के सर्वरों से कनेक्ट होना
- D. असेंबली भाषा में कस्टम प्रोटोकॉल लिखना

4 **4. मैन्युअल OpenVPN बाहरी कॉन्फ़िगरेशन के लिए क्या ज़रूरी है?**

- A. सर्वर कनेक्शन के लिए कस्टम लोगो डिज़ाइन करना
- B. प्रमाणपत्र कुंजियों वाली .ovpn प्रोफ़ाइल इंपोर्ट करना
- C. घर के राउटर की भौतिक जगह बदलना
- D. ऑपरेटिंग सिस्टम फ़ायरवॉल को पूरी तरह अक्षम करना

5 **5. कोई प्रशासक किसी सेटअप में स्प्लिट टनलिंग का उपयोग क्यों करेगा?**

- A. सारा इंटरनेट ट्रैफ़िक पूरी तरह ब्लॉक करना
- B. चुनिंदा सुरक्षित ऐप्स को सुरक्षित टनल बायपास करने देना
- C. भौतिक राउटर को दो अलग इकाइयों में बाँटने के लिए
- D. प्रशासनिक निगरानी के लिए एन्क्रिप्शन अक्षम करने के लिए

चेकपॉइंट 2: सही या गलत चुनौती

6 प्रश्न 6

6. राउटर VPN सेट करना एक सरल प्रक्रिया है जिसमें किसी तकनीकी कौशल की ज़रूरत नहीं होती।

○ सही ○ गलत

7 प्रश्न 7

7. Windows और macOS में IKEv2 और L2TP का समर्थन करने वाले नेटिव क्लाइंट हैं।

○ सही ○ गलत

8 प्रश्न 8

8. WireGuard सेट करने के लिए पब्लिक और प्राइवेट कुंजियाँ जनरेट करनी पड़ती हैं।

○ सही ○ गलत

9 प्रश्न 9

9. VPN टनल आपके स्थानीय नेटवर्क के प्रिंटरों और प्रिंट जॉब को सुरक्षित करती है।

○ सही ○ गलत

10 प्रश्न 10

10. VPN ऐप्स न चला सकने वाले स्मार्ट लॉक को कवर करने के लिए राउटर-स्तर का VPN चाहिए।

○ 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. गेटवे _____ स्तर पर VPN इंस्टॉल करने से स्मार्ट टीवी और गेमिंग कंसोल सुरक्षित रहते हैं।

2. मैनुअल OpenVPN कॉन्फ़िगरेशन में _____ सर्वर प्रोफ़ाइल आयात करनी पड़ती है।

3. ऑपरेटिंग सिस्टम में पहले से मौजूद कॉन्फ़िगरेशन सिस्टम की _____ क्लाइंट सेटिंग का उपयोग करते हैं।

4. WireGuard प्रमाणीकरण क्रिप्टोग्राफ़िक सार्वजनिक और निजी _____ पर निर्भर करता है।

5. उपयोग में आसान इंस्टॉलेशन प्रदाता के आधिकारिक _____ से होता है।

6. केरी को VPN _____ सर्वर से भेजने पर नाम-समाधान ट्रैकिंग लीक रुकते हैं।

शब्दावली शब्द-बैंक

ऐप ओवीपीएन कनेक्शन लॉग्स की पेयर डीएनएस नेटिव राउटर स्प्लिट टनलिंग

अपने उत्तर यहाँ लिखें:

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

चेकपॉइंट 4: नेटवर्क अवधारणा मिलान

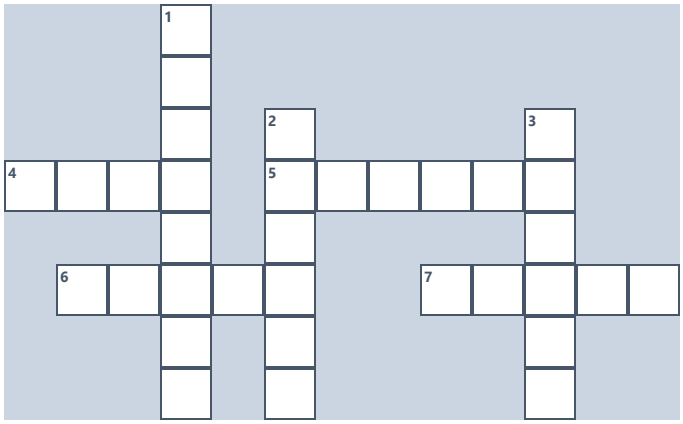
परिभाषा मिलान

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. VPN ऐप**	**A**	स्थानीय नेटवर्क के सभी स्मार्ट उपकरणों को सुरक्षित करने वाला गेटवे-स्तर का एन्क्रिप्शन।
☐	**2. राउटर VPN**	**B**	आसान वन-क्लिक सेटअप के लिए सदस्यता सेवा द्वारा दिया गया सॉफ़्टवेयर पैकेज।
☐	**3. नेटिव क्लाइंट**	**C**	विफल सेटअप को डीबग करने के लिए त्रुटि आउटपुट और क्लाइंट स्टेटस लॉग जाँचना।
☐	**4. .ovpn प्रोफ़ाइल**	**D**	ट्रैफ़िक रूट अलग-अलग करना ताकि कुछ ऐप एन्क्रिप्टेड टनल को बायपास कर सकें।
☐	**5. कुंजी जोड़ी**	**E**	ऐप इंस्टॉल किए बिना मूल ऑपरेटिंग सिस्टम सेटिंग के भीतर ट्रैफ़िक सुरक्षित करना।
☐	**6. स्प्लिट टनलिंग**	**F**	डोमेन लुकअप लीक रोकने के लिए नेटवर्क रिज़ॉल्वर पते कॉन्फ़िगर करना।
☐	**7. DNS सर्वर सेटअप**	**G**	WireGuard हैंडशेक स्थापित करने के लिए आवश्यक क्रिप्टोग्राफ़िक टोकन (सार्वजनिक/निजी)।
☐	**8. कनेक्शन लॉग**	**H**	सर्वर, पोर्ट सेटिंग्स और सर्टिफ़िकेट कुंजियों वाला OpenVPN फ़ाइल फ़ॉर्मेट।

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

4. WireGuard हैंडशेक स्थापित करने के लिए ज़रूरी क्रिप्टोग्राफ़िक टोकन (सार्वजनिक/निजी) (4)

5. ऐप इंस्टॉल किए बिना ऑपरेटिंग सिस्टम की अपनी सेटिंग के भीतर ट्रैफ़िक सुरक्षित करना (6)

6. सर्वर, पोर्ट सेटिंग और सर्टिफ़िकेट कुंजियों वाला OpenVPN फ़ाइल फ़ॉर्मैट (5)

7. डोमेन लुकअप लीक रोकने के लिए नेटवर्क रिज़ॉल्वर पते कॉन्फ़िगर करना (5)

ऊपर से नीचे

1. गेटवे-स्तर का एन्क्रिप्शन, जो लोकल नेटवर्क के सभी स्मार्ट उपकरणों की सुरक्षा करता है (8)

2. असफल सेटअप को डीबग करने के लिए त्रुटि आउटपुट और क्लाइंट स्टेटस लॉग जाँचना (6)

3. ट्रैफ़िक के रास्ते अलग करना, ताकि चुनिंदा ऐप एन्क्रिप्टेड टनल को बायपास करें (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

4 बाएँ से दाएँ: WireGuard हैंडशेक स्थापित करने के लिए ज़रूरी क्रिप्टोग्राफ़िक टोकन (सार्वजनिक/निजी) (4 अक्षर):

5 बाएँ से दाएँ: ऐप इंस्टॉल किए बिना ऑपरेटिंग सिस्टम की अपनी सेटिंग के भीतर ट्रैफ़िक सुरक्षित करना (6 अक्षर):

6 बाएँ से दाएँ: सर्वर, पोर्ट सेटिंग और सर्टिफ़िकेट कुंजियों वाला OpenVPN फ़ाइल फ़ॉर्मेट (5 अक्षर):

7 बाएँ से दाएँ: डोमेन लुकअप लीक रोकने के लिए नेटवर्क रिज़ॉल्वर पते कॉन्फ़िगर करना (5 अक्षर):

ऊपर से नीचे

1 ऊपर से नीचे: गेटवे-स्तर का एन्क्रिप्शन, जो लोकल नेटवर्क के सभी स्मार्ट उपकरणों की सुरक्षा करता है (8 अक्षर):

2 ऊपर से नीचे: असफल सेटअप को डीबग करने के लिए त्रुटि आउटपुट और क्लाइंट स्टेटस लॉग जाँचना (6 अक्षर):

3 ऊपर से नीचे: ट्रैफ़िक के रास्ते अलग करना, ताकि चुनिंदा ऐप एन्क्रिप्टेड टनल को बायपास करें (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।

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

शब्दावली शब्द-सूची

वीपीएनऐप, राउटरवीपीएन, नेटिवक्लाइंट, ओवीपीएन, कीपेयर, स्प्लिटटनलिंग, डीएनएस, कनेक्शनलॉग्स

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. वीपीएनऐप**
- **B. राउटरवीपीएन**
- **C. नेटिवक्लाइंट**
- **D. ओवीपीएन**
- **E. कीपेयर**
- **F. स्प्लिटटनलिंग**
- **G. डीएनएस**
- **H. कनेक्शनलॉग्स**

परिभाषाएँ और मिलान फ़ील्ड

1. डोमेन लुकअप लीक रोकने के लिए नेटवर्क रिज़ॉल्वर पते कॉन्फ़िगर करना।
2. ट्रैफ़िक के रास्ते अलग करना, ताकि चुनिंदा ऐप एन्क्रिप्टेड टनल को बायपास करें।
3. गेटवे-स्तर का एन्क्रिप्शन, जो लोकल नेटवर्क के सभी स्मार्ट उपकरणों की सुरक्षा करता है।
4. WireGuard हैंडशेक स्थापित करने के लिए ज़रूरी क्रिप्टोग्राफ़िक टोकन (सार्वजनिक/निजी)।
5. ऐप इंस्टॉल किए बिना ऑपरेटिंग सिस्टम की अपनी सेटिंग के भीतर ट्रैफ़िक सुरक्षित करना।
6. असफल सेटअप को डीबग करने के लिए त्रुटि आउटपुट और क्लाइंट स्टेटस लॉग जाँचना।
7. सर्वर, पोर्ट सेटिंग और सर्टिफ़िकेट कुंजियों वाला OpenVPN फ़ाइल फ़ॉर्मैट।
8. आसान एक-क्लिक सेटअप के लिए सब्सक्रिप्शन सेवा द्वारा दिया गया सॉफ़्टवेयर पैकेज।

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. **ए वी न ऐ प पी** _____

2. **ट ने व इं क्ला टि** _____

3. **र की य पे** _____

4. **न स ए डी ए** _____

5. **वी पी उ न र रा ए ट** _____

6. **ए ओ पी न वी** _____

7. **लिं स्प्लि न ग ट ट** _____

8. **क्श ग्स क लॉ न ने** _____

अतिरिक्त गतिविधि: झटपट सोचें

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

1	सेट अप होने के बाद जाँचने वाली चीज़ें			
2	ऐसे डिवाइस जो VPN इस्तेमाल कर सकते हैं			
3	आपके जाने-पहचाने VPN सेवाएँ			
4	यात्रा के दौरान VPN इस्तेमाल करने के कारण			
5	सेटअप के दौरान लोगों की गलतियाँ			
6	इस वर्कशीट के वे शब्द जिन्हें आप याद रखना चाहते हैं			
7	ऐसी सेटिंग्स जिन्हें आप सबसे पहले चालू करते हैं			
8	अच्छे VPN प्रदाता के वादे			
9	VPN सेट अप करते समय के चरण			
10	ऐसी जगहें जहाँ आप VPN इस्तेमाल करेंगे			
11	नकली Wi-Fi नेटवर्क पहचानने के तरीके			
12	ऐसी चीज़ें जिन्हें VPN छिपा सकता है			
13	ऐसी चीज़ें जो आपका इंटरनेट प्रदाता देख सकता है			
14	मदद पाने की जगहें			
15	शुरू करने के लिए आपको जिन चीज़ों की ज़रूरत है			

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

अपनी सर्वर कॉन्फ़िगरेशन की ट्रेनिंग पूरी करने के लिए, सुरक्षित टनल सेट करने के बारे में यह छिपा संदेश डिक्रिप्ट करें।

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

15	52	23	41	52		44	49	39	13	61	43	47	28		25	52	37	32
		44	52		3	57	44	61	23	56	40		13	39	52	57		

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: शुरू करने के लिए मुझे क्या चाहिए?

आपको एक सक्रिय VPN सदस्यता या अपना VPN सर्वर, एक समर्थित डिवाइस, और या तो प्रोवाइडर का ऐप या मैन्युअल सेटअप का ब्योरा चाहिए: सर्वर एड्रेस, प्रोटोकॉल और आपके क्रेडेंशियल, कुंजियाँ या प्रमाणपत्र। अधिकांश लोग बस आधिकारिक ऐप इंस्टॉल करते हैं, साइन इन करते हैं और कनेक्ट पर टैप करते हैं।

Q3: मैं ऐप के बिना Windows पर VPN कैसे सेट करूँ?

Settings > Network & internet > VPN खोलें, Add VPN चुनें, और प्रदाता का सर्वर नाम, VPN प्रकार (जैसे IKEv2 या L2TP/IPsec) और अपनी साइन-इन जानकारी दर्ज करें। फिर Connect चुनें।

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: मैं macOS कैसे सेट करूँ?

प्रदाता का macOS ऐप इंस्टॉल करें, या System Settings > VPN खोलें, VPN कॉन्फ़िगरेशन जोड़ें, IKEv2, L2TP over IPSec या Cisco IPSec चुनें, और अपने प्रदाता से मिला सर्वर पता तथा क्रेडेंशियल दर्ज करें।

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: मैं .ovpn फ़ाइल का उपयोग कैसे करूँ?

OpenVPN क्लाइंट इंस्टॉल करें, अपने प्रदाता या एडमिनिस्ट्रेटर से मिली .ovpn प्रोफ़ाइल इम्पोर्ट करें, और कनेक्ट करें। इस फ़ाइल में सर्वर का पता, पोर्ट, UDP या TCP सेटिंग और अक्सर सर्टिफ़िकेट व कुंजियाँ होती हैं।

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।

Q2: मैं WireGuard को मैन्युअल रूप से कैसे सेट करूँ?

wg genkey और wg pubkey से कुंजी जोड़ी बनाएँ, अपनी सार्वजनिक कुंजी सर्वर के साथ साझा करें, और ऐसी कॉन्फ़िग लिखें जिसमें आपकी निजी कुंजी, पीयर की सार्वजनिक कुंजी, allowed IPs और endpoint हों। wg-quick टूल इसे चालू करता है। [2]

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: मैं अपने होम राउटर पर VPN सुरक्षित रूप से कैसे सेट करूँ?

जाँचें कि आपका राउटर VPN क्लाइंट मोड को सपोर्ट करता है, उसके एडमिन पेज में लॉग इन करें और प्रदाता की OpenVPN या WireGuard फ़ाइल अपलोड करें। कुछ राउटरों में पहले फ़र्मवेयर अपडेट करना पड़ता है; उसके बाद नेटवर्क का हर डिवाइस टनल का उपयोग करता 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: मैं कैसे जाँचूँ कि मेरा नया VPN सेटअप काम कर रहा है?

कनेक्ट करें, फिर IP-जाँच वाली साइट पर जाएँ: उसे VPN सर्वर का IP पता और स्थान दिखाना चाहिए। DNS और WebRTC लीक टेस्ट चलाएँ, और कनेक्शन को थोड़ी देर के लिए तोड़कर पुष्टि करें कि किल स्विच ट्रैफ़िक को ब्लॉक करता है।

Q8: सेटअप के बाद अगर मेरा VPN कनेक्ट न हो तो मुझे क्या जाँचना चाहिए?

अपना लॉगिन या कुंजियाँ, सर्वर का पता, और यह जाँचें कि चुना गया पोर्ट और प्रोटोकॉल ब्लॉक नहीं हैं। UDP और TCP के बीच या किसी दूसरे सर्वर पर स्विच करके देखें, और त्रुटियों के लिए ऐप के कनेक्शन लॉग पढ़ें।

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 अपने-आप शुरू होना चाहिए?

आमतौर पर हाँ। ज़्यादातर ऐप स्टार्टअप पर या असुरक्षित Wi-Fi पर अपने-आप चालू होकर कनेक्ट हो सकते हैं, इसलिए दूसरे ऐप के डेटा भेजना शुरू करने से पहले ही आप सुरक्षित रहते हैं।

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. नेटिव क्लाइंट

Windows और macOS दोनों में बिल्ट-इन VPN क्लाइंट हैं जो IKEv2 और L2TP/IPsec का समर्थन करते हैं, इसलिए कई कनेक्शन अतिरिक्त ऐप के बिना सेट अप किए जा सकते हैं।

2. कुंजी निर्माण

WireGuard की क्विक स्टार्ट wg genkey से प्राइवेट कुंजी बनाती है और उससे wg pubkey द्वारा पब्लिक कुंजी निकालती है। [2]

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। [1]

4. प्रोफ़ाइल फ़ाइलें

.ovpn प्रोफ़ाइल सर्वर का पता, पोर्ट, प्रोटोकॉल और सर्टिफ़िकेट को एक साथ जोड़ती है, इसलिए एक इंपोर्ट से OpenVPN कनेक्शन सेट हो जाता है।

5. डिफ़ॉल्ट पोर्ट

OpenVPN आम तौर पर पोर्ट 1194 का उपयोग करता है, जबकि WireGuard के आधिकारिक उदाहरण UDP पोर्ट 51820 का उपयोग करते हैं; टनल कनेक्ट होने के लिए फ़ायरवॉल और राउटर पर इन पोर्ट को अनुमति देनी पड़ सकती है।

6. डीप पैकेट इंस्पेक्शन

डीप पैकेट इंस्पेक्शन (DPI) आम VPN प्रोटोकॉल को पहचानकर ब्लॉक कर सकता है; TCP पोर्ट 443 पर OpenVPN या ऑब्फ़स्केटेड मोड पर जाने से मदद मिल सकती है।

7. राउटर कवरेज

राउटर पर VPN उसके पीछे के हर डिवाइस की सुरक्षा करता है, जिनमें कंसोल और स्मार्ट टीवी भी शामिल हैं जो VPN ऐप नहीं चला सकते, और हर डिवाइस पर कुछ इंस्टॉल करने की ज़रूरत नहीं पड़ती।

8. कीपअलाइव

NAT या फ़ायरवॉल के पीछे WireGuard की PersistentKeepalive सेटिंग, जो आमतौर पर 25 सेकंड होती है, टनल को पहुँच योग्य बनाए रखती है। [2]

9. TUN/TAP ड्राइवर

OpenVPN को TUN/TAP वर्चुअल नेटवर्क इंटरफ़ेस के साथ काम करने के लिए डिज़ाइन किया गया है, जो अधिकांश प्लेटफ़ॉर्म पर उपलब्ध है और क्लाइंट इंस्टॉल करने पर सेट हो जाता है। [3]

10. स्प्लिट टनलिंग

सेटअप के दौरान स्प्लिट टनलिंग आपको चुने हुए ऐप या पतों को VPN से बाहर रखने देती है, जो स्थानीय प्रिंटर या VPN IP पते ब्लॉक करने वाले ऐप के लिए मददगार है।

तकनीकी संदर्भ और स्रोत

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

शैक्षणिक और उद्योग संदर्भ

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

[2] WireGuard. (n.d.). Quick Start.
https://www.wireguard.com/quickstart/

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

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

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

उत्तर कुंजी: Windows, macOS, Android, iOS, Linux और राउटर पर VPN कॉन्फ़िगर करना

1 **प्रश्न 1** सही उत्तर: A

शिक्षण नोट

मोबाइल डिवाइस पर VPN सेट अप करने का सबसे आसान तरीका क्या है? → ऐप स्टोर से आधिकारिक VPN ऐप डाउनलोड करना

2 **राउटर गेटवे सेटअप** लेटेंसी सही उत्तर: B

शिक्षण नोट

राउटर VPN गेटवे पर ट्रैफ़िक को एन्क्रिप्ट करता है और उन IoT उपकरणों, कंसोल और स्मार्ट उपकरणों की सुरक्षा करता है जिनमें मूल VPN ऐप इंस्टॉल करने की क्षमता नहीं होती। संदर्भ: DD-WRT OpenVPN Clients, Linksys Router Config। [3]

3 **प्रश्न 3** सही उत्तर: A

शिक्षण नोट

Windows और macOS में IKEv2 और L2TP/IPsec जैसे प्रोटोकॉल के लिए बिल्ट-इन क्लाइंट होते हैं, इसलिए अतिरिक्त सॉफ़्टवेयर इंस्टॉल किए बिना कनेक्शन सेट अप किया जा सकता है।

4 **OpenVPN प्रोफ़ाइल इम्पोर्ट** रूटिंग नियंत्रण सही उत्तर: B

शिक्षण नोट

मैन्युअल कॉन्फ़िगरेशन में.ovpn प्रोफ़ाइल कुंजियाँ डाउनलोड करनी पड़ती हैं, जिनमें लक्षित सर्वर पोर्ट, प्रोटोकॉल पैरामीटर (UDP/TCP) और क्रिप्टोग्राफ़िक प्रमाणपत्र होते हैं। संदर्भ: DD-WRT OpenVPN Clients।

5 **स्प्लिट टनल रूटिंग** गोपनीयता सही उत्तर: B

शिक्षण नोट

स्प्लिट टनलिंग उपयोगकर्ताओं को संवेदनशील कार्य ऐप एन्क्रिप्टेड टनल से रूट करने देती है, जबकि स्थानीय स्ट्रीमिंग या गेम VPN ओवरहेड के बिना सीधे जुड़ते हैं। उद्धरण: IETF IKEv2 RFC।

उत्तर कुंजी: चेकपॉइंट 2 – सही या गलत

6 **प्रश्न 6**

सही उत्तर: गलत

शिक्षण नोट

राउटर सेटअप का मतलब है एडमिन पेज में लॉग इन करना, VPN सपोर्ट जाँचना और कॉन्फ़िग फ़ाइलें अपलोड करना।

7 **नेटिव OS इंटीग्रेशन** गति

सही उत्तर: सही

शिक्षण नोट

प्रमुख ऑपरेटिंग सिस्टम सुरक्षित कनेक्शन सेटअप आसान बनाने के लिए प्रोटोकॉल का नेटिव इंटीग्रेशन अंदर ही शामिल करते हैं। संदर्भ: Microsoft Native Gateway, Apple Support Profiles।

8 **WireGuard कुंजी जोड़ी** स्निफ़िंग का जोखिम

सही उत्तर: सही

शिक्षण नोट

WireGuard पासवर्ड या CA श्रृंखलाओं पर निर्भर रहने के बजाय सुरक्षित P2P हैंडशेक स्थापित करने के लिए असिमेट्रिक कुंजियों का उपयोग करता है। उद्धरण: WireGuard CLI Specifications।

9 **स्थानीय ट्रैफ़िक ब्लॉक** फ़ायरवॉल

सही उत्तर: गलत

शिक्षण नोट

VPN आमतौर पर सार्वजनिक इंटरनेट ट्रैफ़िक रूट करते हैं, और जब तक अन्यथा कॉन्फ़िगर न किया जाए, कभी-कभी स्थानीय नेटवर्क प्रिंटरों तक पहुँच ब्लॉक कर सकते हैं। उद्धरण: Microsoft Native Gateway।

10 **प्रश्न 10**

सही उत्तर: सही

शिक्षण नोट

VPN ऐप्स न चला सकने वाले स्मार्ट लॉक को कवर करने के लिए राउटर-स्तर का VPN चाहिए।

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. VPN ऐप	A 2. राउटर VPN	E 3. नेटिव क्लाइंट	H 4. .ovpn प्रोफ़ाइल
G 5. कुंजी जोड़ी	D 6. स्प्लिट टनलिंग	F 7. DNS सर्वर सेटअप	C 8. कनेक्शन लॉग

चेकपॉइंट 3: उत्तर – प्रमुख शब्द

1 राउटर	2 ओवीपीएन	3 नेटिव	4 की पेयर
5 ऐप	6 डीएनएस		

चेकपॉइंट 6, वैकल्पिक: उत्तर – शब्द मिलान

1 G – डीएनएस	2 F – स्प्लिटटनलिंग	3 B – राउटरवीपीएन	4 E – कीपेयर
5 C – नेटिवक्लाइंट	6 H – कनेक्शनलॉग्स	7 D – ओवीपीएन	8 A – वीपीएनऐप

शिक्षकों के लिए चर्चा नोट

प्रमुख शब्द:
जाँचें कि क्या विद्यार्थी VPN ऐप, राउटर VPN और नेटिव क्लाइंट 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।

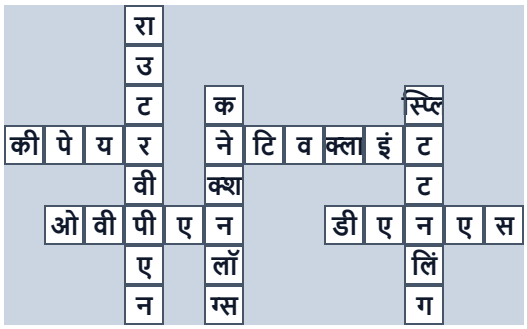
स्रोतों का मूल्यांकन:
विद्यार्थियों से वर्कशीट के स्रोतों में कम से कम एक कथन की पुष्टि करवाएँ और चर्चा करें कि आँकड़े, कीमतें और नियम समय के साथ क्यों बदल सकते हैं।

पहेलियों की कुंजियाँ और शिक्षक नोट

शब्द खोज समाधान

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

क्रॉसवर्ड समाधान



क्रॉसवर्ड समाधान के लिए शिक्षक गाइड

बाएँ से दाएँ

4 बाएँ से दाएँ: कीपेयर WireGuard हैंडशेक स्थापित करने के लिए ज़रूरी क्रिप्टोग्राफ़िक टोकन (सार्वजनिक/निजी) (4 अक्षर)

5 बाएँ से दाएँ: नेटिवक्लाइंट ऐप इंस्टॉल किए बिना ऑपरेटिंग सिस्टम की अपनी सेटिंग के भीतर ट्रैफ़िक सुरक्षित करना (6 अक्षर)

6 बाएँ से दाएँ: ओवीपीएन सर्वर, पोर्ट सेटिंग और सर्टिफ़िकेट कुंजियों वाला OpenVPN फ़ाइल फ़ॉर्मैट (5 अक्षर)

7 बाएँ से दाएँ: डीएनएस डोमेन लुकअप लीक रोकने के लिए नेटवर्क रिज़ॉल्वर पते कॉन्फ़िगर करना (5 अक्षर)

ऊपर से नीचे

1 ऊपर से नीचे: राउटरवीपीएन गेटवे-स्तर का एन्क्रिप्शन, जो लोकल नेटवर्क के सभी स्मार्ट उपकरणों की सुरक्षा करता है (8 अक्षर)

2 ऊपर से नीचे: कनेक्शनलॉग्स असफल सेटअप को डीबग करने के लिए त्रुटि आउटपुट और क्लाइंट स्टेटस लॉग जाँचना (6 अक्षर)

3 ऊपर से नीचे: स्प्लिटटनलिंग ट्रैफ़िक के रास्ते अलग करना, ताकि चुनिंदा ऐप एन्क्रिप्टेड टनल को बायपास करें (6 अक्षर)

अक्षर-फेर शब्द और कूट संदेश हल कुंजी

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

शब्द अनस्क्रैम्बल कुंजी

1. एवीनऐपपी → **वीपीएनऐप**
2. टनेवइंक्लाटि → **नेटिवक्लाइंट**
3. रकीयपे → **कीपेयर**
4. नसएडीए → **डीएनएस**
5. वीपीउनरराएट → **राउटरवीपीएन**
6. एओपीनवी → **ओवीपीएन**
7. लिंस्प्लिनगटट → **स्प्लिटटनलिंग**
8. क्शग्सकलॉनने → **कनेक्शनलॉग्स**

गुप्त कूट चुनौती कुंजी

"गेटवे सुरक्षित डेमन से इंस्टॉल करें"

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।