नाम: _____ दिनांक: _____ अंक: _____

WireGuard बनाम OpenVPN वर्कशीट

WireGuard और OpenVPN प्रोटोकॉल, कोडबेस आकार, गति और क्रिप्टोग्राफ़िक मानकों की तुलना

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

- प्रोटोकॉल की कोडबेस जटिलता और ऑडिट की गति की तुलना करें।
- कर्नेल स्पेस के भीतर चलने से मिलने वाले प्रदर्शन लाभों का विश्लेषण करें।
- OpenSSL सिफ़र की तुलना WireGuard की आधुनिक क्रिप्टोग्राफ़ी से करें।
- पीयर हैंडशेक के लिए पब्लिक और प्राइवेट कुंजी जोड़े सेट करें।
- VPN ट्रैफ़िक को TCP और UDP फ़ायरवॉल पोर्ट से रूट करना।

प्रोटोकॉल तुलना वर्कशीट 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 आधुनिक प्रोटोकॉल के ऑडिट पर लागू करें। अंत में अतिरिक्त गतिविधि झटपट सोचें पूरी करें।

WireGuard बनाम OpenVPN (परिचय)

VPN प्रोटोकॉल चुनने में स्पीड और कॉन्फ़िगरेशन विकल्पों के बीच संतुलन बनाना पड़ता है। OpenVPN दशकों से मानक रहा है और TCP/UDP कॉन्फ़िगरेशन की लचीलापन देता है। WireGuard एक आधुनिक विकल्प है जो सीधे कर्नेल स्पेस में चलता है और जिसमें केवल 4,000 लाइनों का कोड है। प्रोटोकॉल के अंतर समझना आपके सुरक्षित नेटवर्क को अनुकूलित करने की कुंजी है।

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

चेकपॉइंट 1: बहुविकल्पीय चुनौती

1. WireGuard प्रोटोकॉल के कोडबेस का अनुमानित आकार कितना है?
   - A. लगभग 70,000 पंक्तियाँ
   - B. 100,000 से अधिक पंक्तियाँ
   - C. 1,000 से कम पंक्तियाँ
   - D. लगभग 4,000 पंक्तियाँ

2. WireGuard ऑपरेटिंग सिस्टम के किस स्पेस में चलता है?
   - A. यूज़र स्पेस
   - B. कर्नेल स्पेस
   - C. ऐप्लिकेशन स्पेस
   - D. वर्चुअल स्पेस

3. OpenVPN मुख्य रूप से किस क्रिप्टोग्राफ़िक लाइब्रेरी पर निर्भर करता है?
   - A. ChaCha20-Poly1305
   - B. OpenSSL क्रिप्टोग्राफ़िक लाइब्रेरी
   - C. Noise प्रोटोकॉल फ़्रेमवर्क
   - D. प्लेनटेक्स्ट DES एन्कोडिंग

4. OpenVPN की तुलना में WireGuard का एक प्रमुख प्रदर्शन लाभ क्या है?
   - A. तेज़ कनेक्शन हैंडशेक और कम लेटेंसी
   - B. सार्वजनिक IP पतों की आवश्यकता को दरकिनार करके
   - C. पुराने डायल-अप के लिए अंतर्निहित नेटिव समर्थन
   - D. मोबाइल डिवाइस पर शून्य बैटरी ओवरहेड

5. WireGuard पीयर कनेक्शनों को कैसे प्रमाणित करता है?
   - A. मानक उपयोगकर्ता पासवर्ड का आदान-प्रदान करके
   - B. डोमेन पंजीकरण प्रमाणपत्रों की जाँच करके
   - C. स्थिर सार्वजनिक और निजी कुंजी जोड़ियों का उपयोग करके
   - D. हार्डवेयर सीरियल नंबर जाँचकर

चेकपॉइंट 2: सही या गलत चुनौती

6 प्रश्न 6

6. WireGuard का संक्षिप्त कोडबेस उसके ऑडिट को काफ़ी आसान बनाता है।

- ◯ सही
- ◯ गलत

7 प्रश्न 7

7. OpenVPN आम तौर पर WireGuard से तेज़ है क्योंकि वह कर्नेल स्पेस में चलता है।

- ◯ सही
- ◯ गलत

8 प्रश्न 8

8. OpenVPN अत्यधिक कॉन्फ़िगर करने योग्य है और UDP तथा TCP दोनों प्रोटोकॉल को सपोर्ट करता है।

- ◯ सही
- ◯ गलत

9 प्रश्न 9

9. WireGuard तेज़ पैकेट एन्क्रिप्शन के लिए ChaCha20 जैसी आधुनिक क्रिप्टोग्राफ़ी का उपयोग करता है।

- ◯ सही
- ◯ गलत

10 प्रश्न 10

10. WireGuard को प्रमाणीकरण के लिए जटिल सर्टिफ़िकेट अथॉरिटी सेटअप की ज़रूरत होती 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. आधुनिक _____ प्रोटोकॉल सीधे OS कर्नेल के भीतर चलता है।
2. पुराना _____ प्रोटोकॉल OpenSSL क्रिप्टो लाइब्रेरी पर निर्भर है।
3. _____ में कोड चलाने से कॉन्टेक्स्ट स्विचिंग का बोझ घटता है।
4. OpenVPN _____ में चलता है और पैकेटों को वर्चुअल इंटरफ़ेस से भेजता है।
5. WireGuard कनेक्शन पीयर की पहचान के लिए सार्वजनिक और निजी _____ का उपयोग करता है।
6. छोटा कोडबेस होने से प्रोसेसिंग का अतिरिक्त _____ कम रहता है।

शब्दावली शब्द-बैंक

ओपन एसएसएल · ओपनवीपीएन · ओवरहेड · कर्नेल स्पेस · की पेयर · यूज़र स्पेस · वर्चुअल इंटरफ़ेस · वायरगार्ड

अपने उत्तर यहाँ लिखें:

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

चेकपॉइंट 4: नेटवर्क अवधारणा मिलान

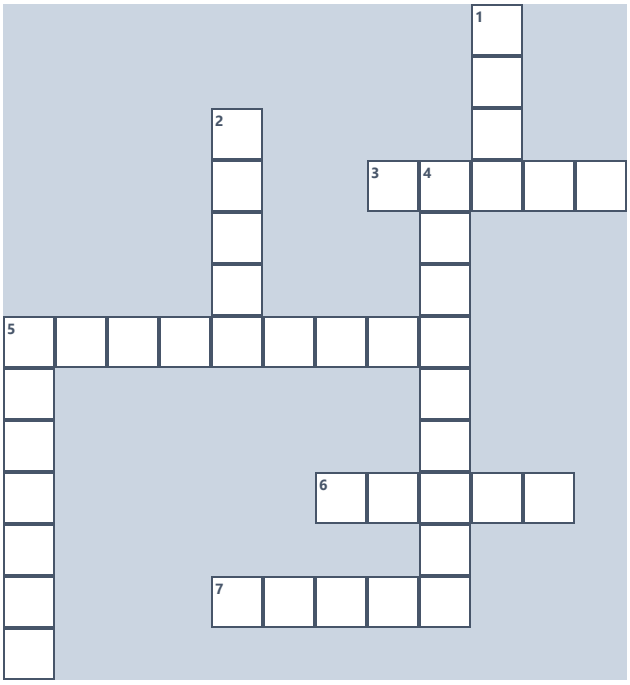
परिभाषा मिलान

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. WireGuard**	**A**	वह निष्पादन क्षेत्र जहाँ OpenVPN चलता है, जिससे कॉन्टेक्स्ट स्विच का ओवरहेड बनता है।
☐	**2. OpenVPN**	**B**	WireGuard कोडबेस का छोटा आकार, जिससे उसका ऑडिट करना कहीं आसान हो जाता है।
☐	**3. कर्नेल स्पेस**	**C**	वह क्रिप्टोग्राफ़िक लाइब्रेरी जिस पर OpenVPN सिफ़र एल्गोरिदम के लिए निर्भर करता है।
☐	**4. यूज़र स्पेस**	**D**	OpenVPN द्वारा समर्थित ट्रांसपोर्ट प्रोटोकॉल; WireGuard स्वयं केवल UDP पर चलता है।
☐	**5. 4,000 पंक्तियाँ**	**E**	ऑपरेटिंग सिस्टम का वह निष्पादन क्षेत्र जहाँ गति के लिए WireGuard चलता है।
☐	**6. OpenSSL**	**F**	WireGuard द्वारा पीयर कनेक्शन सत्यापित करने के लिए इस्तेमाल होने वाले असममित टोकन।
☐	**7. कुंजी जोड़ी**	**G**	आधुनिक VPN प्रोटोकॉल, जो तेज़ गति और सरल कोड ऑडिट के लिए बना है।
☐	**8. TCP/UDP**	**H**	बड़े, जटिल कॉन्फ़िगरेशन कोडबेस वाला मज़बूत पुराना प्रोटोकॉल।

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. सुरक्षा या प्रोसेसिंग के कारण जुड़ने वाला अतिरिक्त बोझ। (5)

5. ओपनवीपीएन जिस पुरानी क्रिप्टोग्राफ़ी लाइब्रेरी पर टिका है। (9)

6. तेज़ गति और सरल कोड ऑडिट के लिए बनाया गया आधुनिक VPN प्रोटोकॉल (5)

7. वह निष्पादन क्षेत्र, जहाँ OpenVPN चलता है और कॉन्टेक्स्ट स्विच ओवरहेड पैदा करता है (5)

ऊपर से नीचे

1. असममित टोकन, जिनका उपयोग WireGuard पीयर कनेक्शन सत्यापित करने के लिए करता है (4)

2. ऑपरेटिंग सिस्टम का वह निष्पादन क्षेत्र, जहाँ WireGuard गति के लिए चलता है (5)

4. सॉफ़्टवेयर द्वारा बनाया गया नेटवर्क पोर्ट, जिससे पैकेट गुज़रते हैं। (9)

5. बड़े, जटिल कॉन्फ़िगरेशन कोडबेस वाला मज़बूत पुराना प्रोटोकॉल (7)

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: सुरक्षा या प्रोसेसिंग के कारण जुड़ने वाला अतिरिक्त बोझ। (5 अक्षर):

5 बाएँ से दाएँ: ओपनवीपीएन जिस पुरानी क्रिप्टोग्राफ़ी लाइब्रेरी पर टिका है। (9 अक्षर):

6 बाएँ से दाएँ: तेज़ गति और सरल कोड ऑडिट के लिए बनाया गया आधुनिक VPN प्रोटोकॉल (5 अक्षर):

7 बाएँ से दाएँ: वह निष्पादन क्षेत्र, जहाँ OpenVPN चलता है और कॉन्टेक्स्ट स्विच ओवरहेड पैदा करता है (5 अक्षर):

ऊपर से नीचे

1 ऊपर से नीचे: असममित टोकन, जिनका उपयोग WireGuard पीयर कनेक्शन सत्यापित करने के लिए करता है (4 अक्षर):

2 ऊपर से नीचे: ऑपरेटिंग सिस्टम का वह निष्पादन क्षेत्र, जहाँ WireGuard गति के लिए चलता है (5 अक्षर):

4 ऊपर से नीचे: सॉफ़्टवेयर द्वारा बनाया गया नेटवर्क पोर्ट, जिससे पैकेट गुज़रते हैं। (9 अक्षर):

5 ऊपर से नीचे: बड़े, जटिल कॉन्फ़िगरेशन कोडबेस वाला मज़बूत पुराना प्रोटोकॉल (7 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।

र	दे	कि	जा	सा	वा	ड	यू	रे	स	ख	नि	फ	ढ	मा
ना	का	रे	दे	सि	मी	क	ज़	ओ	पि	ता	ति	ज	श	भ
ऊ	अ	र	ऊ	ए	रि	वि	र	श	प	य	वि	व	वा	पा
स	ल	य	च	से	कि	य	स्पे	घ	प	न	के	की	व	सि
फ़े	री	पे	त	की	ओ	कि	स	सि	ना	ओ	वी	ने	पा	ते
र	ण	की	ए	ता	प	सा	मी	न	नी	ऋ	व	पी	ले	घ
ट	ति	जि	ला	ए	न	जी	ले	क	ड	ल	द	र	ए	जे
इं	घ	के	च	से	ए	दे	री	नें	ए	पी	उ	अ	हे	न
ल	जे	मि	घ	व	स	आ	च	ल	मी	च	ट	थ	फ	ड
अ	ग	ना	सी	का	ए	ज	फ	स्पे	नी	जी	ता	ठ	से	लि
र्चु	ट	आ	इ	से	स	रा	के	स	री	पा	वा	सि	य	वा
व	नि	पि	ने	ख	ए	के	वे	ऊ	ड	नी	दे	दि	य	भ
आ	नि	जे	वे	वे	ल	ष	ण	प	कि	से	य	र	ह	ह
ते	रा	द	सा	सी	थ	जे	इ	मे	ला	ढ	गा	पे	ऋ	वे
नी	वे	उ	थ	ह	जे	त	य	मी	रे	र्ड	मि	दि	ए	ह

शब्दावली शब्द-सूची

वायरगार्ड · ओपनवीपीएन · कर्नेलस्पेस · यूज़रस्पेस · कीपेयर · ओवरहेड · ओपनएसएसएल · वर्चुअलइंटरफ़ेस

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. वायरगार्ड**
- **B. ओपनवीपीएन**
- **C. कर्नेलस्पेस**
- **D. यूज़रस्पेस**
- **E. कीपेयर**
- **F. ओवरहेड**
- **G. ओपनएसएसएल**
- **H. वर्चुअलइंटरफ़ेस**

परिभाषाएँ और मिलान फ़ील्ड

1. सुरक्षा या प्रोसेसिंग के कारण जुड़ने वाला अतिरिक्त बोझ।
2. ऑपरेटिंग सिस्टम का वह निष्पादन क्षेत्र, जहाँ WireGuard गति के लिए चलता है।
3. बड़े, जटिल कॉन्फ़िगरेशन कोडबेस वाला मज़बूत पुराना प्रोटोकॉल।
4. ओपनवीपीएन जिस पुरानी क्रिप्टोग्राफ़ी लाइब्रेरी पर टिका है।
5. सॉफ़्टवेयर द्वारा बनाया गया नेटवर्क पोर्ट, जिससे पैकेट गुज़रते हैं।
6. असममित टोकन, जिनका उपयोग WireGuard पीयर कनेक्शन सत्यापित करने के लिए करता है।
7. तेज़ गति और सरल कोड ऑडिट के लिए बनाया गया आधुनिक VPN प्रोटोकॉल।
8. वह निष्पादन क्षेत्र, जहाँ OpenVPN चलता है और कॉन्टेक्स्ट स्विच ओवरहेड पैदा करता है।

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. गा र वा र्ड य
2. क स स्पे ल र्ने
3. र की य पे
4. स ल ए ए स ए ओ प न
5. पी न वी न ओ ए प
6. स्पे यू र स ज़
7. हे ड ओ र व
8. स इं फ़े व ल चुं ट र अ

अतिरिक्त गतिविधि: झटपट सोचें

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

1	WireGuard चुनने के कारण			
2	अच्छे VPN प्रदाता के वादे			
3	OpenVPN चुनने के कारण			
4	यात्रा के दौरान VPN इस्तेमाल करने के कारण			
5	ऐसी चीज़ें जो आपका इंटरनेट प्रदाता देख सकता है			
6	नकली Wi-Fi नेटवर्क पहचानने के तरीके			
7	VPN के बारे में मिथक			
8	ऐसी जगहें जहाँ आप VPN इस्तेमाल करेंगे			
9	रोज़मर्रा की ज़िंदगी की तेज़ चीज़ें			
10	ऐसी चीज़ें जिनसे VPN आपको नहीं बचा सकता			
11	ऐसी चीज़ें जो कोड की जाँच आसान बनाती हैं			
12	ऐसी चीज़ें जिन्हें VPN छिपा सकता है			
13	WireGuard और OpenVPN के बीच अंतर			
14	गोपनीयता से जुड़े शब्द			
15	आपके जाने-पहचाने एन्क्रिप्शन के नाम			

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 कैफ़े के Wi-Fi पर हूँ और मेरा VPN ऐप मुझे WireGuard या OpenVPN चुनने देता है। जब मैं कैफ़े नेटवर्क और अपने फ़ोन के हॉटस्पॉट के बीच चलता हूँ तो मेरी वीडियो कॉल बार-बार कट जाती हैं। मुझे कौन-सा प्रोटोकॉल चुनना चाहिए, और वह इस बदलाव को बेहतर तरीके से कैसे संभालेगा?"

Alex (यात्री छात्र)

👩‍🦲 "मैं विदेश में एक होटल नेटवर्क पर हूँ जो ज़्यादातर VPN ट्रैफ़िक ब्लॉक करता लगता है। WireGuard बिल्कुल कनेक्ट नहीं हो रहा, लेकिन मुझे घर पर अपने स्कूल के संसाधनों तक पहुँचना है। संभवतः क्या ब्लॉक किया जा रहा है, और OpenVPN मुझे इससे निकलने में कैसे मदद कर सकता है?"

चेकपॉइंट 9: कूट संदेश को डिकोड करें

अपनी प्रोटोकॉल ऑडिटिंग की ट्रेनिंग पूरी करने के लिए, कर्नेल-स्पेस में निष्पादन 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

28	52	20	60		23	32	40		44	52		10	33	32	41	48	33	48	8	32

1	33	15	61	39	52	25		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: प्रोटोकॉल क्यों मायने रखते हैं?

प्रोटोकॉल तय करता है कि आपका VPN अपनी टनल कैसे बनाता है, कौन-सी क्रिप्टोग्राफ़ी आपके डेटा की रक्षा करती है, और वह कितनी तेज़ी से कनेक्ट और दोबारा कनेक्ट होता है। WireGuard और OpenVPN वे दो ओपन-सोर्स प्रोटोकॉल हैं जो अधिकतर VPN ऐप देते हैं, और वे सरलता, गति और कॉन्फ़िगर करने की सुविधा के बीच अलग-अलग समझौते करते हैं।

Q3: क्या उनमें से कोई एक दूसरे से अधिक निजी है?

कोई भी प्रोटोकॉल आपको गुमनाम नहीं बनाता। दोनों मज़बूत सिफ़र से टनल ट्रैफ़िक को एन्क्रिप्ट करते हैं; आपकी गोपनीयता ज़्यादातर इस पर निर्भर करती है कि VPN प्रदाता क्या लॉग करता है और कुंजियों, खातों तथा सर्वरों को कैसे संभालता 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 दोनों ओपन सोर्स हैं?

हाँ। WireGuard और OpenVPN कम्युनिटी एडिशन दोनों अपना सोर्स कोड प्रकाशित करते हैं, इसलिए स्वतंत्र शोधकर्ता उनकी समीक्षा कर सकते हैं। WireGuard का छोटा कोडबेस पूरी समीक्षा को कहीं तेज़ बना देता है।

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: इनमें से कौन तेज़ है?

WireGuard आम तौर पर अधिक तेज़ होता है: यह कर्नेल में चलता है, हल्के ChaCha20-Poly1305 एन्क्रिप्शन का उपयोग करता है और हैंडशेक जल्दी पूरा करता है। OpenVPN में ओवरहेड अधिक होता है, लेकिन वास्तविक गति सर्वर लोड और दूरी पर भी निर्भर करती है।

Q7: क्या दोनों TCP और UDP पर चल सकते हैं?

नहीं। OpenVPN UDP या TCP पर चल सकता है, और TCP मोड उन नेटवर्क पर मदद करता है जो UDP ब्लॉक करते हैं। WireGuard अपने पैकेट केवल UDP पर भेजता है, इसलिए यह उन नेटवर्क पर विफल हो सकता है जो केवल TCP की अनुमति देते हैं। [4]

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 पर WireGuard और OpenVPN उपयोग कर सकता हूँ?

हाँ। WireGuard क्रॉस-प्लेटफ़ॉर्म है, जिसके ऐप्स Windows, macOS, Linux, iOS और Android के लिए हैं, और OpenVPN क्लाइंट भी इन्हीं सिस्टम पर हैं। अधिकांश VPN ऐप्स में आप इनमें से कोई भी चुन सकते हैं। [1]

Q10: WireGuard इतना छोटा क्यों है?

WireGuard कई विकल्पों के बजाय आधुनिक सिफ़र का एक निश्चित सेट समर्थित करता है। इसके Linux कार्यान्वयन में 4,000 से कम कोड लाइनें लगती हैं, जिससे बड़े VPN कोडबेस की तुलना में इसका ऑडिट आसान होता है। [3]

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: WireGuard कौन-से सिफ़र उपयोग करता है?

WireGuard एन्क्रिप्शन के लिए ChaCha20 के साथ Poly1305, कुंजी विनिमय के लिए Curve25519, हैशिंग के लिए BLAKE2s और हैंडशेक के लिए Noise फ़्रेमवर्क का उपयोग करता है। इसमें सिफ़र की बातचीत नहीं होती, इसलिए उपयोगकर्ता कोई कमज़ोर विकल्प नहीं चुन सकते। [2]

Q3: OpenVPN कौन-से सिफ़र और लाइब्रेरी उपयोग कर सकता है?

OpenVPN, OpenSSL लाइब्रेरी के साथ कसकर एकीकृत है और कुंजियों के आदान-प्रदान के लिए TLS का उपयोग करता है। एडमिनिस्ट्रेटर AES-256-GCM जैसे डेटा-चैनल सिफ़र चुन सकते हैं, जिससे लचीलापन मिलता है लेकिन कमज़ोर सेटिंग्स की गुंजाइश भी बनती है। [4]

Q4: प्रत्येक प्रोटोकॉल पीयर को कैसे प्रमाणित करता है?

WireGuard पीयर स्थिर पब्लिक कुंजियों से एक-दूसरे को पहचानते हैं, बिल्कुल SSH कुंजियाँ बदलने की तरह, और हर कुंजी अनुमत टनल IP से जुड़ी होती है। OpenVPN आम तौर पर X.509 सर्टिफ़िकेट वाली सर्टिफ़िकेट अथॉरिटी पर निर्भर करता है, जिसे अक्सर यूज़रनेम और पासवर्ड के साथ जोड़ा 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: जब मैं Wi-Fi से मोबाइल नेटवर्क पर स्विच करता हूँ तो क्या होता है?

WireGuard कनेक्शनलेस है: यह नए पते से पैकेट भेजता है और तेज़ हैंडशेक के बाद टनल चलती रहती है। OpenVPN सत्र की स्थिति रखता है, इसलिए नेटवर्क बदलने पर दोबारा कनेक्ट करना पड़ सकता है, जिसमें थोड़ा अधिक समय लगता है।

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: अगर WireGuard तेज़ है तो क्या OpenVPN अब भी अच्छा विकल्प है?

हाँ। OpenVPN परिपक्व है और व्यापक रूप से तैनात है, UDP ब्लॉक होने पर TCP पर चलता है, और प्रमाणपत्र-आधारित एंटरप्राइज़ सेटअप को सपोर्ट करता है। कई प्रोवाइडर दोनों प्रोटोकॉल देते हैं, ताकि एक के ब्लॉक या धीमा होने पर उपयोगकर्ता बदल सकें।

Q9: वे कौन-से पोर्ट उपयोग करते हैं?

OpenVPN का मानक पोर्ट 1194 है, लेकिन उसे 443 समेत किसी भी UDP या TCP पोर्ट पर ले जाया जा सकता है। WireGuard अपनी कॉन्फ़िगरेशन में तय किए गए UDP पोर्ट पर सुनता है; उसके आधिकारिक उदाहरणों में 51820 पोर्ट इस्तेमाल होता है।

Q10: कौन-सा प्रोटोकॉल हाथ से सेट करना आसान है?

WireGuard आम तौर पर अधिक सरल है: कुंजी जोड़ी बनाएँ, पब्लिक कुंजियाँ बदलें और अनुमत IP की सूची बनाएँ। OpenVPN को सर्टिफ़िकेट, CA और अधिक विकल्पों की ज़रूरत होती है, हालाँकि .ovpn प्रोफ़ाइल इन्हें एक फ़ाइल में जोड़ देती 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. 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. दो ट्रांसपोर्ट

OpenVPN अपनी टनल UDP या TCP पर चला सकता है, और TLS मोड में इसके कंट्रोल और डेटा चैनल एक ही पोर्ट साझा करते हैं। [4]

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। [3]

4. आधुनिक क्रिप्टोग्राफ़ी

WireGuard, Noise प्रोटोकॉल फ़्रेमवर्क के भीतर ChaCha20, Poly1305, Curve25519, BLAKE2s, SipHash24 और HKDF को जोड़ता है, जिसमें उपयोगकर्ताओं के लिए चुनने को कोई सिफ़र नहीं है जिससे गलती हो। [2]

5. OpenVPN के भीतर OpenSSL

OpenVPN, OpenSSL लाइब्रेरी के साथ कसकर एकीकृत है और अपनी कई क्रिप्टोग्राफ़िक क्षमताएँ उसी से लेता है, जिसमें कुंजियों के आदान-प्रदान के लिए इस्तेमाल होने वाला TLS भी शामिल है। [4]

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. SSH-शैली की कुंजियाँ

WireGuard कनेक्शन साधारण पब्लिक कुंजियाँ आपस में बदलकर सेट अप होते हैं, बिल्कुल SSH कुंजियाँ बदलने की तरह, और किसी सर्टिफ़िकेट अथॉरिटी की ज़रूरत नहीं होती। [1]

8. क्रॉस-प्लेटफ़ॉर्म

WireGuard पहले Linux कर्नेल के लिए जारी हुआ था और अब Windows, macOS, BSD, iOS तथा Android के लिए उपलब्ध है, इसलिए वही प्रोटोकॉल अधिकांश डिवाइस पर काम करता है। [1]

9. फ़ॉरवर्ड सीक्रेसी

लंबी अवधि की कुंजी बाद में लीक हो जाए तब भी परफ़ेक्ट फ़ॉरवर्ड सीक्रेसी देने के लिए, WireGuard सिमेट्रिक सत्र कुंजियाँ बदलने हेतु हर कुछ मिनट में अपना Noise_IK हैंडशेक दोहराता है। [2]

10. TUN/TAP इंटरफ़ेस

OpenVPN को TUN/TAP वर्चुअल नेटवर्क इंटरफ़ेस के साथ काम करने के लिए डिज़ाइन किया गया है, जो अधिकांश प्लेटफ़ॉर्म पर उपलब्ध है और टनल के पैकेट वहन करता है। [4]

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.). Protocol & Cryptography.
https://www.wireguard.com/protocol/

[3] 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/

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

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

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

उत्तर कुंजी: WireGuard और OpenVPN प्रोटोकॉल, कोडबेस आकार, गति और क्रिप्टोग्राफ़िक मानकों की तुलना

1 **WireGuard कोड आकार** प्रोटोकॉल — **सही उत्तर: D**

शिक्षण नोट

WireGuard अत्यंत संक्षिप्त है और लगभग 4,000 कोड लाइनों पर चलता है। इससे आक्रमण सतह छोटी रहती है और ऑडिट आसान हो जाता है। उद्धरण: WireGuard Project।

2 **कर्नेल स्पेस की गति** लेटेंसी — **सही उत्तर: B**

शिक्षण नोट

कर्नेल स्पेस में सीधे चलकर WireGuard कॉन्टेक्स्ट स्विचिंग का ओवरहेड टाल देता है, जिससे उच्च थ्रूपुट संभव होता है। उद्धरण: WireGuard Project।

3 **प्रश्न 3** — **सही उत्तर: B**

शिक्षण नोट

OpenVPN, OpenSSL के साथ गहराई से जुड़ा है, जो AES-GCM जैसे सिफ़र देता है; इससे वह बहुत कॉन्फ़िगर करने योग्य बनता है लेकिन ज़्यादा जटिल भी।

4 **प्रोटोकॉल प्रदर्शन** रूटिंग नियंत्रण — **सही उत्तर: A**

शिक्षण नोट

WireGuard मिलीसेकंड में हैंडशेक स्थापित करता है और नेटवर्क रोमिंग (जैसे Wi-Fi से सेलुलर पर स्विच करना) पर तुरंत प्रतिक्रिया देता है। उद्धरण: Microsoft Native Gateway, Apple Support। [3]

5 **असममित क्रिप्टोग्राफ़ी** गोपनीयता — **सही उत्तर: C**

शिक्षण नोट

WireGuard, SSH सेटअप कॉन्फ़िगरेशन की तरह, पब्लिक कुंजियों को अनुमत टनल IP पतों से जोड़ने वाली Cryptokey Routing का उपयोग करता है। उद्धरण: WireGuard Project।

उत्तर कुंजी: चेकपॉइंट 2 – सही या गलत

6 **प्रश्न 6** — **सही उत्तर: सही**

शिक्षण नोट

WireGuard का Linux इम्प्लीमेंटेशन 4,000 पंक्तियों से कम है, इसलिए सुरक्षा टीमें OpenVPN जैसे कहीं बड़े VPN कोडबेस की तुलना में उसकी समीक्षा बहुत तेज़ी से कर सकती हैं।

7 **यूज़र स्पेस लेटेंसी** गति — **सही उत्तर: गलत**

शिक्षण नोट

OpenVPN यूज़र स्पेस में चलता है और पैकेट को कर्नेल वर्चुअल इंटरफ़ेस से आगे-पीछे भेजता है, जिससे कॉन्टेक्स्ट-स्विच ओवरहेड बढ़ता है (जब तक OpenVPN DCO जैसा कर्नेल ऑफ़लोड इस्तेमाल न हो)। उद्धरण: DD-WRT custom firmware.

8 **OpenVPN कॉन्फ़िगरेशन** स्निफ़िंग का जोखिम — **सही उत्तर: सही**

शिक्षण नोट

OpenVPN, TCP (भरोसेमंदी/फ़ायरवॉल बायपास के लिए) या UDP (गति के लिए) पर चल सकता है, जिससे वह जटिल एंटरप्राइज़ फ़ायरवॉल के साथ संगत रहता है। उद्धरण: IETF Cryptographic Protocols.

9 **आधुनिक क्रिप्टोग्राफ़ी** फ़ायरवॉल — **सही उत्तर: सही**

शिक्षण नोट

WireGuard पुराने सिफ़र छोड़कर ChaCha20 और Poly1305 जैसे आधुनिक, सुरक्षित मूल तत्वों को अपनाता है, जो मोबाइल CPU पर तेज़ चलते हैं। उद्धरण: WireGuard Project।

10 **की पेयर का सरलीकरण** नो-लॉग्स — **सही उत्तर: गलत**

शिक्षण नोट

WireGuard सर्टिफ़िकेट या जटिल CA पदानुक्रम का उपयोग नहीं करता; यह पीयर के बीच बदली गई साधारण पब्लिक/प्राइवेट कुंजी जोड़ियों पर निर्भर करता है। उद्धरण: WireGuard Project।

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

G 1. WireGuard	H 2. OpenVPN	E 3. कर्नेल स्पेस	A 4. यूज़र स्पेस
B 5. 4,000 पंक्तियाँ	C 6. OpenSSL	F 7. कुंजी जोड़ी	D 8. TCP/UDP

चेकपॉइंट 3: उत्तर – प्रमुख शब्द

1 वायरगार्ड	2 ओपनवीपीएन	3 कर्नेल स्पेस	4 यूज़र स्पेस
5 की पेयर	6 ओवरहेड		

चेकपॉइंट 6, वैकल्पिक: उत्तर – शब्द मिलान

1 F – ओवरहेड	2 C – कर्नेलस्पेस	3 B – ओपनवीपीएन	4 G – ओपनएसएसएल
5 H – वर्चुअलइंटरफ़ेस	6 E – कीपेयर	7 A – वायरगार्ड	8 D – यूज़रस्पेस

शिक्षकों के लिए चर्चा नोट

प्रमुख शब्द:
जाँचें कि क्या विद्यार्थी WireGuard, OpenVPN और कर्नेल स्पेस 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

र	दे	कि	जा	सा	वा	ड	यू	रे	स	ख	नि	फ	ढ	मा
ना	का	रे	दे	सि	मी	क	ज़	ओ	पि	ता	ति	ज	श	भ
ऊ	अ	र	ऊ	ए	रि	वि	र	श	प	य	वि	व	वा	पा
स	ल	य	च	से	कि	य	स्पे	घ	प	न	के	की	व	सि
फ़े	री	पे	त	की	ओ	कि	स	सि	ना	ओ	वी	ने	पा	ते
र	ण	की	ए	ता	प	सा	मी	न	नी	ऋ	व	पी	ले	घ
ट	ति	जि	ला	ए	न	जी	ले	क	ड	ल	द	र	ए	जे
इं	घ	के	च	से	ए	दे	री	नें	ए	पी	उ	अ	हे	न
ल	जे	मि	घ	व	स	आ	च	ल	मी	च	ट	थ	फ	ड
अ	ग	ना	सी	का	ए	ज	फ	स्पे	नी	जी	ता	ठ	से	लि
चुं	ट	आ	इ	से	स	रा	के	स	री	पा	वा	सि	य	वा
व	नि	पि	ने	ख	ए	के	वे	ऊ	ड	नी	दे	दि	य	भ
आ	नि	जे	वे	वे	ल	ष	ण	प	कि	से	य	र	ह	ह
ते	रा	द	सा	सी	थ	जे	इ	मे	ला	ढ	गा	पे	ऋ	वे
नी	वे	उ	थ	ह	जे	त	य	मी	रे	र्ड	मि	दि	ए	ह

क्रॉसवर्ड समाधान



क्रॉसवर्ड समाधान के लिए शिक्षक गाइड

बाएँ से दाएँ

3 बाएँ से दाएँ: ओवरहेड सुरक्षा या प्रोसेसिंग के कारण जुड़ने वाला अतिरिक्त बोझ। (5 अक्षर)

5 बाएँ से दाएँ: ओपनएसएसएल ओपनवीपीएन जिस पुरानी क्रिप्टोग्राफ़ी लाइब्रेरी पर टिका है। (9 अक्षर)

6 बाएँ से दाएँ: वायरगार्ड तेज़ गति और सरल कोड ऑडिट के लिए बनाया गया आधुनिक VPN प्रोटोकॉल (5 अक्षर)

7 बाएँ से दाएँ: यूज़रस्पेस वह निष्पादन क्षेत्र, जहाँ OpenVPN चलता है और कॉन्टेक्स्ट स्विच ओवरहेड पैदा करता है (5 अक्षर)

ऊपर से नीचे

1 ऊपर से नीचे: कीपेयर असममित टोकन, जिनका उपयोग WireGuard पीयर कनेक्शन सत्यापित करने के लिए करता है (4 अक्षर)

2 ऊपर से नीचे: कर्नेलस्पेस ऑपरेटिंग सिस्टम का वह निष्पादन क्षेत्र, जहाँ WireGuard गति के लिए चलता है (5 अक्षर)

4 ऊपर से नीचे: वर्चुअलइंटरफ़ेस सॉफ़्टवेयर द्वारा बनाया गया नेटवर्क पोर्ट, जिससे पैकेट गुज़रते हैं। (9 अक्षर)

5 ऊपर से नीचे: ओपनवीपीएन बड़े, जटिल कॉन्फ़िगरेशन कोडबेस वाला मज़बूत पुराना प्रोटोकॉल (7 अक्षर)

अक्षर-फेर शब्द और कूट संदेश हल कुंजी

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

शब्द अनस्क्रैम्बल कुंजी

1. गारवार्डय — **वायरगार्ड**
2. कसस्पेलर्नें — **कर्नेलस्पेस**
3. रकीयपे — **कीपेयर**
4. सलएएसएओपन — **ओपनएसएसएल**
5. पीनवीनओएप — **ओपनवीपीएन**
6. स्पेयूरसज़ — **यूज़रस्पेस**
7. हेडओरव — **ओवरहेड**
8. सइंफ़ेवलर्चुटरअ — **वर्चुअलइंटरफ़ेस**

गुप्त कूट चुनौती कुंजी

"तेज़ टनल से ओपनवीपीएन अपग्रेड करें"

केस स्टडी के उत्तर

A परिदृश्य A: प्रोटोकॉल चुनना

स्ट्रिमिंग और एन्क्रिप्शन सारा की दुविधा

ग्रेडिंग दिशानिर्देश

छात्रों के उत्तरों में निम्नलिखित बिंदु शामिल होने चाहिए:

- अनुशंसा: WireGuard। इसका हल्का, कनेक्शनलेस डिज़ाइन नेटवर्क बदलने पर टनल को तेज़ी से बहाल होने देता है, और ChaCha20-Poly1305 एन्क्रिप्शन को तेज़ रखता है।
- सुरक्षा: दोनों प्रोटोकॉल कैफ़े के Wi-Fi पर उसके ट्रैफ़िक को एन्क्रिप्ट करते हैं, इसलिए सही ढंग से कॉन्फ़िगर होने पर कोई भी उसके लॉगिन की सुरक्षा करता है; चुनाव मुख्यतः स्पीड और स्थिरता को प्रभावित करता है।

B परिदृश्य B: VPN ब्लॉक को पार करना

जियो-ब्लॉकिंग और IP Alex की दुविधा

ग्रेडिंग दिशानिर्देश

छात्रों के उत्तरों में निम्नलिखित बिंदु शामिल होने चाहिए:

- ब्लॉक होने का कारण: WireGuard केवल UDP का उपयोग करता है, और होटल का फ़ायरवॉल संभवतः UDP को ब्लॉक करता है या फ़िल्टरिंग अथवा डीप पैकेट इंस्पेक्शन के ज़रिए WireGuard पैकेट पहचान लेता है।
- OpenVPN कैसे मदद करता है: यह TCP पर चल सकता है, जिसमें HTTPS द्वारा उपयोग किया जाने वाला पोर्ट 443 भी शामिल है, जिसे होटल के फ़ायरवॉल शायद ही पूरी तरह ब्लॉक करते हैं क्योंकि वेब ब्राउज़िंग उसी पर निर्भर है।