नाम: _____ दिनांक: _____ अंक: _____

VPN कैसे चुनें वर्कशीट

VPN प्रदाताओं, सुरक्षा मानकों, ऑडिट और लॉगिंग नीतियों का मूल्यांकन

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

- गोपनीयता के लिए प्रदाता के क्षेत्राधिकार और ज़ीरो-लॉग्स नीतियों का मूल्यांकन करें।
- गति के लिए WireGuard और OpenVPN जैसे टनलिंग प्रोटोकॉल की तुलना करें।
- किल स्विच और केवल RAM वाले सर्वर नोड जैसी सुरक्षा सुविधाओं का विश्लेषण करें।
- चुनते समय स्वतंत्र सुरक्षा ऑडिट और प्राइसिंग प्लान की पहचान करें।
- अपनी स्पीड और जियो-अनब्लॉकिंग की ज़रूरतों के आधार पर सर्वर स्थान चुनें।

चयन 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 सुरक्षित VPN इंफ्रास्ट्रक्चर चुनने पर लागू करें। अंत में अतिरिक्त गतिविधि झटपट सोचें पूरी करें।

VPN का चयन (परिचय)

सही VPN चुनने के लिए मार्केटिंग के दावों से आगे देखना ज़रूरी है। एक भरोसेमंद प्रदाता के पास सिद्ध ज़ीरो-लॉग्स नीति, सुरक्षित एन्क्रिप्शन प्रोटोकॉल और ओपन-सोर्स क्लाइंट होने चाहिए। सुरक्षा सुविधाओं, अधिकार क्षेत्र और गति प्रदर्शन का मूल्यांकन करके आप ऐसा VPN चुन सकते हैं जो आपकी डिजिटल सुरक्षा ज़रूरतों के अनुरूप हो।

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

चेकपॉइंट 1: बहुविकल्पीय चुनौती

1. सुरक्षित VPN प्रदाता चुनते समय मुख्य कारक क्या है?
   - A. सर्वर वाले देशों की संख्या
   - B. स्वतंत्र रूप से ऑडिट की गई नो-लॉग्स नीति
   - C. सबसे कम मासिक मूल्य स्तर
   - D. भड़कीले विज्ञापन प्रायोजन

2. कौन-सा VPN प्रोटोकॉल गति और ऑडिट-योग्यता का सबसे अच्छा संतुलन देता है?
   - A. PPTP (पुराना)
   - B. L2TP/IPSec
   - C. केवल TCP पर OpenVPN
   - D. WireGuard

3. संवेदनशील गतिविधियों के लिए उपयोगकर्ताओं को मुफ़्त VPN से क्यों बचना चाहिए?
   - A. संयुक्त राज्य अमेरिका में उन पर प्रतिबंध है
   - B. वे अक्सर आपका वेब ब्राउज़िंग इतिहास बेच देते हैं
   - C. वे बुनियादी वेब ब्राउज़िंग को सपोर्ट नहीं करते
   - D. उनसे जुड़ने के लिए विशेष हार्डवेयर चाहिए

4. किसी प्रदाता का मूल कानूनी क्षेत्राधिकार क्या निर्धारित करता है?
   - A. सर्वर कनेक्शन की गति
   - B. समर्थित डिवाइसों के प्रकार
   - C. डेटा प्रतिधारण और तलाशी वारंट से जुड़े स्थानीय कानून
   - D. क्लाइंट ऐप्लिकेशन की विज़ुअल थीम

5. VPN क्लाइंट की 'किल स्विच' सुविधा का मुख्य उद्देश्य क्या है?
   - A. VPN कनेक्शन टूटने पर इंटरनेट पहुँच ब्लॉक करना
   - B. डिवाइस पर इंस्टॉल किए गए सभी ऐप्लिकेशन मिटाना
   - C. सर्वर कनेक्शन की गति दोगुनी करने के लिए
   - D. निष्क्रिय होने पर ऑपरेटिंग सिस्टम को रीस्टार्ट करने के लिए

चेकपॉइंट 2: सही या गलत चुनौती

6 प्रश्न 6

6. VPN आपके डिवाइस को मैलवेयर डाउनलोड और वायरस फ़ाइलों से बचाता है।

○ सही ○ गलत

7 प्रश्न 7

7. Deloitte जैसी फ़र्मों के स्वतंत्र ऑडिट ज़ीरो-लॉग के दावों को सत्यापित करते हैं।

○ सही ○ गलत

8 प्रश्न 8

8. प्रदाता के गृह देश के कानून उपयोगकर्ता डेटा की गोपनीयता को प्रभावित नहीं करते।

○ सही ○ गलत

9 प्रश्न 9

9. WireGuard का संक्षिप्त कोडबेस OpenVPN के कोडबेस की तुलना में ऑडिट करने में आसान है।

○ सही ○ गलत

10 प्रश्न 10

10. मुफ़्त VPN अक्सर सर्वर लागत निकालने के लिए विज्ञापन बेचते हैं या उपयोगकर्ताओं को ट्रैक करते हैं।

○ 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. स्वतंत्र रूप से सत्यापित _____ नीति VPN प्रदाता को आपका ऑनलाइन इतिहास दर्ज न करने के लिए प्रतिबद्ध करती है।

2. आधुनिक _____ प्रोटोकॉल उच्च गति देता है और बहुत छोटे कोडबेस का उपयोग करता है।

3. जितना बड़ा और फैला हुआ _____ होगा, उतने ही अधिक देशों से कनेक्ट करना संभव होगा।

4. वीपीएन चालू होने पर मिलने वाली _____ स्ट्रीमिंग और गेमिंग के अनुभव को तय करती है।

5. _____ डिस्क से सर्वर सुरक्षित करने से रीबूट के बाद उपयोगकर्ता डेटा के बने रहने से बचने में मदद मिलती है।

6. ज़ीरो-नॉलेज दावे वाली नीति की पुष्टि के लिए प्रतिष्ठित फ़र्मों से तृतीय-पक्ष सुरक्षा _____ ज़रूरी है।

शब्दावली शब्द-बैंक

ऑडिट कनेक्शन गति क्षेत्राधिकार नो-लॉग्स रैम-ओनली वायरगार्ड सर्वर नेटवर्क OPENVPN

अपने उत्तर यहाँ लिखें:

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

चेकपॉइंट 4: नेटवर्क अवधारणा मिलान

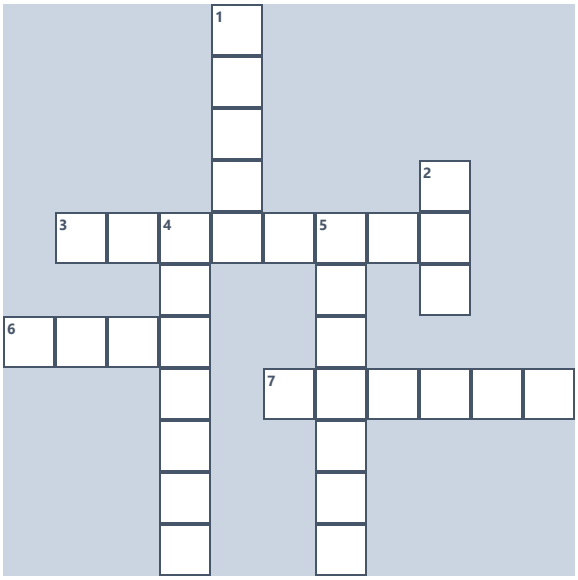
परिभाषा मिलान

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**	उच्च जोखिम वाली कनेक्शन सेवा जो अक्सर लॉगिंग और ब्राउज़र डेटा बेचकर कमाई करती है।
☐	**2. ऑडिट किए गए लॉग**	**B**	सुरक्षा तंत्र, जो सुरक्षित टनल कटने पर इंटरनेट रूटिंग रोक देता है।
☐	**3. क्षेत्राधिकार**	**C**	US, UK, CA, AU और NZ के बीच अंतरराष्ट्रीय खुफ़िया जानकारी साझा करने वाला गठबंधन।
☐	**4. किल स्विच**	**D**	हार्डवेयर इन्फ्रास्ट्रक्चर जो वोलेटाइल मेमोरी पर चलता है, इसलिए डेटा डिस्क पर संग्रहीत नहीं होता।
☐	**5. फ़ाइव आइज़**	**E**	वह भौगोलिक क्षेत्र जो VPN प्रदाता के कानूनी दायित्व तय करता है।
☐	**6. मुफ़्त VPN**	**F**	आधुनिक, तेज़ प्रोटोकॉल, जो लगभग 4,000 पंक्तियों के अत्यंत ऑडिट-योग्य कोड का उपयोग करता है।
☐	**7. केवल RAM वाले सर्वर**	**G**	परिपक्व, व्यापक रूप से ऑडिट किया गया ओपन-सोर्स प्रोटोकॉल, जिसका कोडबेस WireGuard से कहीं बड़ा है।
☐	**8. OpenVPN**	**H**	स्वतंत्र तृतीय-पक्ष साइबर सुरक्षा फ़र्मों द्वारा सत्यापित गोपनीयता दावा।

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. स्थायी डिस्क के बिना चलने वाला सर्वर (8)

6. जानकारी को कूट-भाषा में बदलने की प्रक्रिया (4)

7. वीपीएन चालू होने पर मिलने वाली इंटरनेट रफ़्तार (6)

ऊपर से नीचे

1. बिना शुल्क वाली वीपीएन सेवा (5)

2. ऑनलाइन ख़तरों से बचाव (3)

4. पुराना, भरोसेमंद खुला-स्रोत वीपीएन प्रोटोकॉल (7)

5. अलग-अलग जगहों पर फैले सर्वरों का जाल (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: स्थायी डिस्क के बिना चलने वाला सर्वर (8 अक्षर):

6 बाएँ से दाएँ: जानकारी को कूट-भाषा में बदलने की प्रक्रिया (4 अक्षर):

7 बाएँ से दाएँ: वीपीएन चालू होने पर मिलने वाली इंटरनेट रफ़्तार (6 अक्षर):

ऊपर से नीचे

1 ऊपर से नीचे: बिना शुल्क वाली वीपीएन सेवा (5 अक्षर):

2 ऊपर से नीचे: ऑनलाइन ख़तरों से बचाव (3 अक्षर):

4 ऊपर से नीचे: पुराना, भरोसेमंद खुला-स्रोत वीपीएन प्रोटोकॉल (7 अक्षर):

5 ऊपर से नीचे: अलग-अलग जगहों पर फैले सर्वरों का जाल (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।

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

वायरगार्ड · फ़्रीवीपीएन · रैमओनलीसर्वर · ओपनवीपीएन · सुरक्षा · एन्क्रिप्शन · सर्वरनेटवर्क · कनेक्शनगति

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. फ़्रीवीपीएन
C. रैमओनलीसर्वर
D. ओपनवीपीएन
E. सुरक्षा
F. एन्क्रिप्शन
G. सर्वरनेटवर्क
H. कनेक्शनगति

परिभाषाएँ और मिलान फ़ील्ड	
	1. ऑनलाइन ख़तरों से बचाव।
	2. आधुनिक, तेज़ और हल्का वीपीएन प्रोटोकॉल।
	3. वीपीएन चालू होने पर मिलने वाली इंटरनेट रफ़्तार।
	4. जानकारी को कूट-भाषा में बदलने की प्रक्रिया।
	5. पुराना, भरोसेमंद खुला-स्रोत वीपीएन प्रोटोकॉल।
	6. अलग-अलग जगहों पर फैले सर्वरों का जाल।
	7. स्थायी डिस्क के बिना चलने वाला सर्वर।
	8. बिना शुल्क वाली वीपीएन सेवा।

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. न रै र म र्व स ली ओ
3. क्षा र सु
4. र्क र्व ट ने व स र
5. पी न फ़्री ए वी
6. ए न पी ओ वी न प
7. प्रा ए न क्रि
8. क्श ति क ग न ने

अतिरिक्त गतिविधि: झटपट सोचें

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

1	ऐसी चीज़ें जिन्हें VPN छिपा सकता है			
2	ऐसी चीज़ें जो कीमत से ज़्यादा मायने रखती हैं			
3	VPN रिव्यू पढ़ने की जगहें			
4	ऐसी चीज़ें जिनसे VPN आपको नहीं बचा सकता			
5	VPN सेल्स टीम के लिए सवाल			
6	ऐसी चीज़ें जो आपका इंटरनेट प्रदाता देख सकता है			
7	VPN चुनते समय आपकी चेकलिस्ट की चीज़ें			
8	ऐसी जगहें जहाँ आप VPN इस्तेमाल करेंगे			
9	VPN प्रदाता में चेतावनी के संकेत			
10	गोपनीयता से जुड़े शब्द			
11	ऐसी चीज़ें जिन्हें आप सबसे पहले जाँचेंगे			
12	अच्छे VPN प्रदाता के वादे			
13	यात्रा के दौरान VPN इस्तेमाल करने के कारण			
14	ऐसे डिवाइस जो VPN इस्तेमाल कर सकते हैं			
15	VPN के बारे में मिथक			

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 चयन गाइड की ट्रेनिंग पूरी करने के लिए, सुरक्षित इन्फ्रास्ट्रक्चर चुनने 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

39	47	33	54	39	61	23		13	48		28	49	40	32	46

44	49	39	13	61	43	47	28		44	47	44	61	23	37		44	52

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: यह पैसा कैसे कमाता है?

बिज़नेस मॉडल जाँचें। सदस्यता, फ़्रीमियम टियर और डेटा बिक्री, सभी यह प्रभावित करते हैं कि आप VPN पर कितना भरोसा कर सकते हैं, और जो सेवा आपका डेटा कभी इकट्ठा ही नहीं करती, वह उसे बेच नहीं सकती। पहले गोपनीयता नीति पढ़ें। [1]

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।

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 पैकेट को ऐसा रूप देता है कि वे सामान्य HTTPS वेब ट्रैफ़िक (पोर्ट 443) जैसे दिखें। इससे सरकारों या स्कूल/ऑफ़िस नेटवर्क द्वारा VPN रोकने के लिए इस्तेमाल की जाने वाली डीप पैकेट इंस्पेक्शन (DPI) को पार करने में मदद मिलती 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: यह जाँचना क्यों ज़रूरी है कि VPN कौन चलाता है और कौन उसका समर्थन करता है?

प्रतिष्ठा मायने रखती है। भरोसा करने से पहले कंपनी के मालिकों और नेताओं के बारे में शोध करें, सार्वजनिक तृतीय-पक्ष ऑडिट खोजें, और देखें कि स्वतंत्र सुरक्षा विशेषज्ञ और प्रेस क्या कहते हैं। [1]

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), जो 1990 के दशक में Microsoft के नेतृत्व वाले समूह का शुरुआती VPN प्रोटोकॉल था, अब असुरक्षित माना जाता है, इसलिए आधुनिक VPN WireGuard या OpenVPN का उपयोग करते हैं। [1]

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। [3]

4. सख़्त ऑडिटिंग मानक

शीर्ष VPN प्रदाता नो-लॉग्स दावों की जाँच के लिए Deloitte, KPMG या PwC जैसी फ़र्मों को, और अपने ऐप व सर्वरों के परीक्षण के लिए Cure53 जैसी सुरक्षा फ़र्मों को नियुक्त करते हैं। [4]

5. 5-Eyes गठबंधन की उत्पत्ति

अमेरिका, ब्रिटेन, कनाडा, ऑस्ट्रेलिया और न्यूज़ीलैंड की Five Eyes खुफ़िया साझेदारी मित्र राष्ट्रों के बीच द्वितीय विश्व युद्ध के समय के सिग्नल्स-इंटेलिजेंस सहयोग से विकसित हुई।

6. डीप पैकेट इंस्पेक्शन

उन्नत फ़ायरवॉल नेटवर्क पैकेट मेटाडेटा का विश्लेषण करने और मानक VPN कनेक्शन की विशेषताओं को ब्लॉक करने के लिए Deep Packet Inspection (DPI) लगाते हैं।

7. कॉर्पोरेट उपयोग

कई संगठन दूरस्थ कर्मचारियों को डेटाबेस जैसे आंतरिक सिस्टम तक पहुँचने के लिए VPN देते हैं, जिससे VPN कार्यस्थल का एक आम सुरक्षा टूल बन जाता 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) गोपनीयता बढ़ाने के लिए ट्रैफ़िक को तीन स्वयंसेवी रिले (गार्ड, मिडिल, एग्ज़िट) से भेजता है। [5]

10. डेटा उल्लंघनों की लागत

VPN को ज़ीरो-ट्रस्ट एक्सेस मॉडल के साथ जोड़ने से, जो हर उपयोगकर्ता और डिवाइस की जाँच करता है, संगठनों को डेटा सुरक्षित रखने और डेटा उल्लंघनों के नुकसान को सीमित करने 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] Electronic Frontier Foundation. (2026). Choosing the VPN That's Right for You.
https://ssd.eff.org/module/choosing-vpn-thats-right-you

[2] Federal Trade Commission. (2018). FTC Provides Tips for Using VPN Apps.
https://www.ftc.gov/news-events/news/press-releases/2018/02/ftc-provides-tips-using-vpn-apps

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

[4] Yahoo Finance. (2026). NordVPN passes its no-logs assurance assessment for the sixth time.
https://finance.yahoo.com/news/nordvpn-passes-no-logs-assurance-140000101.html

[5] Tor Project. (n.d.). Overview.
https://support.torproject.org/about-tor/how-tor-works/overview/

उत्तर कुंजी: VPN प्रदाताओं, सुरक्षा मानकों, ऑडिट और लॉगिंग नीतियों का मूल्यांकन

1 ऑडिट किए गए लॉग की नीति

प्रोटोकॉल

सही उत्तर: B

शिक्षण नोट

स्वतंत्र रूप से ऑडिट की गई नो-लॉग्स नीति किसी प्रदाता के ज़ीरो-नॉलेज गोपनीयता दावों को जाँचने का सबसे व्यावहारिक तरीका है। भड़कीली मार्केटिंग या स्व-दावे पर्याप्त नहीं हैं। संदर्भ: Deloitte Advisory, Cure53 Audit।

2 WireGuard की श्रेष्ठता

लेटेंसी

सही उत्तर: D

शिक्षण नोट

WireGuard कर्नेल स्पेस में आधुनिक, तेज़ कनेक्शन रूटिंग देता है और इसका कोडबेस संक्षिप्त (~4,000 लाइनें) है, जिससे ऑडिट बहुत कुशल हो जाते हैं। उद्धरण: IETF Protocol RFC, WireGuard Project।

3 प्रश्न 3

सही उत्तर: B

शिक्षण नोट

मुफ़्त VPN को भी सर्वरों का खर्च उठाना पड़ता है, और FTC चेतावनी देता है कि कुछ VPN ऐप उपयोगकर्ता डेटा तीसरे पक्षों के साथ साझा करते हैं, जैसे विज्ञापन दिखाने के लिए।

4 कानूनी क्षेत्राधिकार

रूटिंग नियंत्रण

सही उत्तर: C

शिक्षण नोट

क्षेत्राधिकार तय करता है कि VPN निगरानी कानूनों, स्थानीय डेटा रिटेंशन आदेशों और गुप्त सरकारी सबपीना वारंट के अधीन है या नहीं। उद्धरण: Privacy Rights Clearinghouse।

5 Kill Switch सुरक्षा

गोपनीयता

सही उत्तर: A

शिक्षण नोट

टनल टूटते ही kill switch सिस्टम नेटवर्क एडाप्टर की रूटिंग तुरंत काट देता है, जिससे असली IP और DNS के उजागर होने वाले लीक रुकते हैं। उद्धरण: IETF Tunnel RFC।

उत्तर कुंजी: चेकपॉइंट 2 – सही या गलत

6 **मैलवेयर की सीमाएँ** IP मास्किंग — **सही उत्तर: गलत**

शिक्षण नोट

VPN एक सुरक्षित एन्क्रिप्टेड पाइपलाइन देता है, लेकिन वह पेलोड या फ़ाइलों को स्कैन नहीं करता। मैलवेयर को ब्लॉक करने के लिए एंटीवायरस सॉफ़्टवेयर ज़रूरी है। संदर्भ: Deloitte Advisory।

7 **स्वतंत्र ऑडिटिंग** गति — **सही उत्तर: सही**

शिक्षण नोट

ऑडिट रिपोर्ट सर्वर सॉफ़्टवेयर कॉन्फ़िगरेशन, केवल-RAM सेटअप के अनुपालन और लॉगिंग डेटाबेस के अभाव की पुष्टि करती हैं। उद्धरण: Deloitte Advisory, Cure53 Audit।

8 **प्रश्न 8** — **सही उत्तर: गलत**

शिक्षण नोट

प्रदाताओं को अपने मूल देश के कानूनों का पालन करना होता है, जिनमें डेटा-रिटेंशन नियम और उनके पास मौजूद डेटा सौंपने के आदेश शामिल हो सकते हैं।

9 **प्रोटोकॉल कोडबेस का आकार** फ़ायरवॉल — **सही उत्तर: सही**

शिक्षण नोट

छोटा कोडबेस संभावित हमले की सतह घटाता है और सुरक्षा टीमों के लिए प्रोटोकॉल की अखंडता सत्यापित करना आसान बनाता है। संदर्भ: WireGuard Project।

10 **विज्ञापन मुद्रीकरण** नो-लॉग्स — **सही उत्तर: सही**

शिक्षण नोट

सब्सक्रिप्शन शुल्क के बिना, मुफ़्त VPN राजस्व कमाने के लिए डेटा माइनिंग, ट्रैफ़िक प्रोफ़ाइलिंग और ब्राउज़र विज्ञापन इंजेक्शन पर निर्भर करते हैं। उद्धरण: 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

F 1. WireGuard	H 2. ऑडिट किए गए लॉग	E 3. क्षेत्राधिकार	B 4. किल स्विच
C 5. फ़ाइव आइज़	A 6. मुफ़्त VPN	D 7. केवल RAM वाले सर्वर	G 8. OpenVPN

चेकपॉइंट 3: उत्तर – प्रमुख शब्द

1 नो-लॉग्स	2 वायरगार्ड	3 सर्वर नेटवर्क	4 कनेक्शन गति
5 रैम-ओनली	6 ऑडिट		

चेकपॉइंट 6, वैकल्पिक: उत्तर – शब्द मिलान

1 E – सुरक्षा	2 A – वायरगार्ड	3 H – कनेक्शनगति	4 F – एन्क्रिप्शन
5 D – ओपनवीपीएन	6 G – सर्वरनेटवर्क	7 C – रैमओनलीसर्वर	8 B – फ़्रीवीपीएन

शिक्षकों के लिए चर्चा नोट

प्रमुख शब्द:
जाँचें कि क्या विद्यार्थी WireGuard, ऑडिट किए गए लॉग और क्षेत्राधिकार 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।

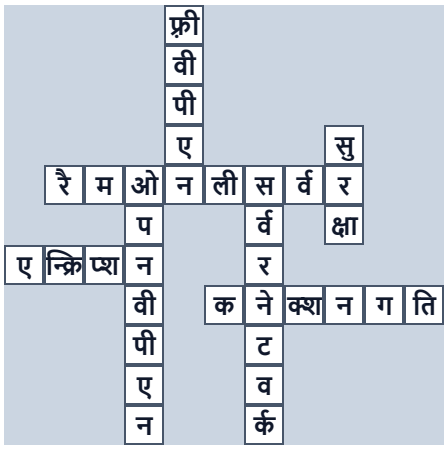
स्रोतों का मूल्यांकन:
विद्यार्थियों से वर्कशीट के स्रोतों में कम से कम एक कथन की पुष्टि करवाएँ और चर्चा करें कि आँकड़े, कीमतें और नियम समय के साथ क्यों बदल सकते हैं।

पहेलियों की कुंजियाँ और शिक्षक नोट

शब्द खोज समाधान

जा	सा	वा	ड	रे	स	ख	**वा**	नि	फ	ढ	मा	ना	का	रे
दे	सि	मी	क	पि	ता	ति	**य**	**क**	ज	श	भ	ऊ	अ	ऊ
ए	रि	**न**	वि	श	य	वि	**र**	व	**ने**	वा	पा	ल	च	से
कि	य	**प्श**	घ	प	के	की	**गा**	व	सि	**क्श**	री	त	की	कि
सि	ना	**न्क्रि**	ने	पा	**रै**	ते	**र्ड**	ण	ए	**फ़्री**	**न**	ता	सा	मी
र्क	न	**ए**	नी	ऋ	**म**	ले	**ओ**	घ	ति	जि	**वी**	**ग**	ला	ए
व	जी	ले	ड	ल	**ओ**	द	जे	**प**	घ	के	च	**पी**	**ति**	से
ट	दे	री	ए	पी	**न**	उ	अ	जे	**न**	मि	घ	व	**ए**	आ
ने	च	मी	च	ट	**ली**	थ	फ	ग	ना	**वी**	सी	का	ज	**न**
र	फ	नी	जी	ता	**स**	ठ	से	लि	ट	आ	**पी**	इ	से	रा
र्व	के	री	पा	वा	**र्व**	सि	य	नि	पि	ने	ख	**ए**	के	वे
स	ऊ	ड	नी	दे	**र**	दि	भ	आ	**क्षा**	नि	जे	वे	**न**	वे
ष	ण	प	कि	से	य	ह	ह	**र**	ते	रा	द	सा	सी	थ
जे	इ	मे	ला	ढ	पे	ऋ	**सु**	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: रैमओनलीसर्वर स्थायी डिस्क के बिना चलने वाला सर्वर (8 अक्षर)

6 बाएँ से दाएँ: एन्क्रिप्शन जानकारी को कूट-भाषा में बदलने की प्रक्रिया (4 अक्षर)

7 बाएँ से दाएँ: कनेक्शनगति वीपीएन चालू होने पर मिलने वाली इंटरनेट रफ़्तार (6 अक्षर)

ऊपर से नीचे

1 ऊपर से नीचे: फ़्रीवीपीएन बिना शुल्क वाली वीपीएन सेवा (5 अक्षर)

2 ऊपर से नीचे: सुरक्षा ऑनलाइन ख़तरों से बचाव (3 अक्षर)

4 ऊपर से नीचे: ओपनवीपीएन पुराना, भरोसेमंद खुला-स्रोत वीपीएन प्रोटोकॉल (7 अक्षर)

5 ऊपर से नीचे: सर्वरनेटवर्क अलग-अलग जगहों पर फैले सर्वरों का जाल (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. नरैरमर्वसलीओ — **रैमओनलीसर्वर**
3. क्षारसु — **सुरक्षा**
4. कर्वटनेवसर — **सर्वरनेटवर्क**
5. पीनफ़्रीएवी — **फ़्रीवीपीएन**
6. एनपीओवीनप — **ओपनवीपीएन**
7. प्शएनक्रि — **एन्क्रिप्शन**
8. क्शतिकगनने — **कनेक्शनगति**

गुप्त कूट चुनौती कुंजी

"रिपोर्ट की तुलना सुरक्षित सिस्टम से"

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।