नाम: _____ दिनांक: _____ अंक: _____

IPVanish समीक्षा

US-मुख्यालय वाले IPVanish VPN का तकनीकी विश्लेषण, मुख्यतः स्वयं के स्वामित्व वाला सर्वर

IPVANISH समीक्षा का शिक्षण 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 IPVanish की तकनीकी समीक्षा से परिचित कराता है। आप स्व-स्वामित्व वाले भौतिक इन्फ्रास्ट्रक्चर, P2P टॉरेंटिंग के लिए SOCKS5 प्रॉक्सी, WireGuard प्रदर्शन और अमेरिकी क्षेत्राधिकार के डेटा नियमों का अध्ययन करेंगे।

वर्कशीट चेकपॉइंट

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

VPN.com सर्वश्रेष्ठ VPN गाइड खोलें

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

आपका IPVanish लर्निंग रोडमैप

- IPVanish Review की तकनीकी संरचना और एन्क्रिप्शन मानकों का विश्लेषण करें।
- IP, DNS और WebRTC ट्रैफ़िक लीक रोकने के लिए क्लाइंट सेटिंग्स कॉन्फ़िगर करें।
- स्वामित्व वाले टनलिंग प्रोटोकॉल की तुलना मानक कार्यान्वयनों से करें।

IPVANISH समीक्षा 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 SOCKS5 प्रॉक्सी और स्वामित्व वाले सर्वर इंफ्रास्ट्रक्चर पर लागू करें। अंत में अतिरिक्त गतिविधि झटपट सोचें पूरी करें।

स्वामित्व वाला इंफ़्रास्ट्रक्चर और SOCKS5 P2P प्रॉक्सी (परिचय)

IPVanish अपने भौतिक सर्वर नेटवर्क के बड़े हिस्से का मालिक होने और उसका प्रबंधन करने के कारण अलग दिखता है, जिससे प्रदर्शन और सुरक्षा बेहतर होती है। यह उच्च गति वाला WireGuard प्रोटोकॉल और P2P टोरेंटिंग के लिए SOCKS5 प्रॉक्सी देता है, लेकिन अमेरिकी Five Eyes क्षेत्राधिकार में काम करता है।

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

चेकपॉइंट 1: बहुविकल्पीय चुनौती

1. 1. IPVanish क्लाइंट ऐप्स में हाई-स्पीड के लिए कौन-सा ओपन-सोर्स प्रोटोकॉल डिफ़ॉल्ट है?
   - A) WireGuard
   - B) L2TP/IPSec
   - C) PPTP
   - D) Catapult Hydra

2. 2. P2P टॉरेंटिंग सेटअप में मदद के लिए IPVanish किस प्रकार का सर्वर प्रॉक्सी देता है?
   - A) SOCKS5 प्रॉक्सी
   - B) HTTP प्रॉक्सी
   - C) Tor रिले
   - D) Shadowsocks

3. 3. 2022 में IPVanish का पहला स्वतंत्र नो-लॉग्स ऑडिट किस फ़र्म ने किया?
   - A) Leviathan Security Group
   - B) PwC
   - C) Deloitte
   - D) Cure53

4. 4. IPVanish की कॉर्पोरेट इकाइयाँ किस प्रमुख राष्ट्रीय क्षेत्राधिकार के तहत काम करती हैं?
   - A) संयुक्त राज्य अमेरिका
   - B) स्विट्ज़रलैंड
   - C) पनामा
   - D) ब्रिटिश वर्जिन आइलैंड्स

5. 5. प्रीमियम IPVanish प्लान के तहत कितने एक साथ डिवाइस कनेक्शन की अनुमति है?
   - A) असीमित
   - B) पाँच
   - C) दस
   - D) सात

चेकपॉइंट 2: सही या गलत चुनौती

6 प्रश्न 6

6. IPVanish अपने भौतिक सर्वर इन्फ्रास्ट्रक्चर के बड़े हिस्से का प्रबंधन करता है और उसका मालिक है।

○ सही ○ गलत

7 प्रश्न 7

7. SOCKS5 प्रॉक्सी ट्रैफ़िक मानक VPN टनल की तरह ट्रांज़िट में पूरी तरह एन्क्रिप्टेड होता है।

○ सही ○ गलत

8 प्रश्न 8

8. IPVanish डेस्कटॉप क्लाइंट में सिस्टम-स्तर का Kill Switch नहीं है।

○ सही ○ गलत

9 प्रश्न 9

9. IPVanish संयुक्त राज्य अमेरिका से संचालित होता है, जो Five Eyes खुफ़िया गठबंधन का सदस्य है।

○ सही ○ गलत

10 प्रश्न 10

10. IPVanish में स्प्लिट टनलिंग ऐप ट्रैफ़िक को VPN टनल के बाहर रूट करने देती 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 बेहतर रूटिंग प्रदर्शन के लिए डिफ़ॉल्ट रूप से कॉन्फ़िगर है।
2. P2P ट्रैफ़िक को असली क्लाइंट स्थान छिपाने के लिए तेज़ _____ से भेजा जा सकता है।
3. नज़दीकी भौगोलिक नोड से जुड़ने पर वास्तविक _____ अधिकतम होती है।
4. IPVanish के उपयोगकर्ता कनेक्शन के लिए अपनी पसंद का _____ चुन सकते हैं।
5. सार्वजनिक वाईफ़ाई पर भी IPVanish आपको एक _____ उपलब्ध कराता है।
6. वीपीएन चालू होने पर मिलने वाली _____ स्ट्रीमिंग के अनुभव को तय करती है।

शब्दावली शब्द-बैंक

कनेक्शन गति | डिवाइस सीमा | वायरगार्ड | सर्वर गति | सर्वर स्थान | सुरक्षित कनेक्शन | KILL SWITCH | SOCKS5 प्रॉक्सी

अपने उत्तर यहाँ लिखें:

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

चेकपॉइंट 4: VPN और नेटवर्क अवधारणा मिलान

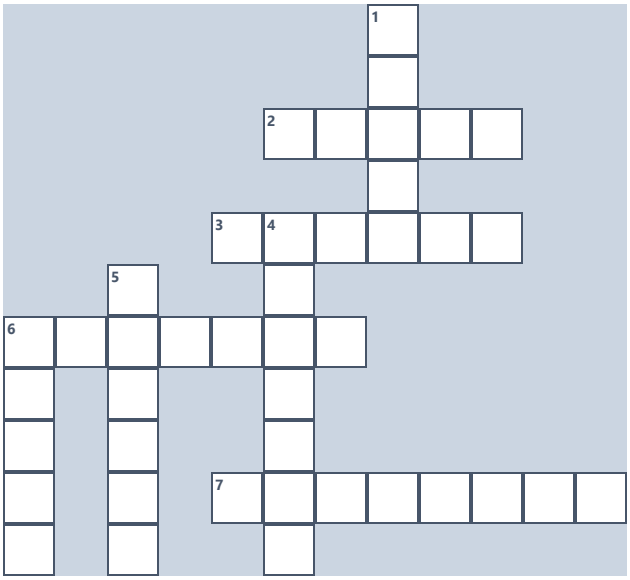
परिभाषा मिलान

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**	फ़ेलसेफ़ तंत्र जो VPN विफल होने पर इंटरनेट ट्रैफ़िक को ब्लॉक करता है।
☐	**2. SOCKS5 प्रॉक्सी**	**B**	गति और आधुनिक क्रिप्टोग्राफ़ी के लिए जाना जाने वाला ओपन-सोर्स प्रोटोकॉल।
☐	**3. सर्वर स्पीड**	**C**	सक्रिय डिवाइस सत्रों की संख्या को सीमित करने वाली बाध्यता।
☐	**4. Kill Switch**	**D**	सक्रिय ट्रैफ़िक लोड में किसी सर्वर नोड की थ्रूपुट क्षमता।
☐	**5. ऑडिट किए गए लॉग**	**E**	इंटरनेट पर डिवाइसों को दिया गया अद्वितीय नेटवर्क पहचानकर्ता।
☐	**6. डिवाइस सीमा**	**F**	एन्क्रिप्टेड टनल सिस्टम की समग्र सुरक्षा स्थिति।
☐	**7. IP पता**	**G**	सत्यापित रिकॉर्ड, जो पुष्टि करते हैं कि उपयोगकर्ता की कोई गतिविधि ट्रैक नहीं होती।
☐	**8. सुरक्षा**	**H**	P2P क्लाइंट के स्थान छिपाने के लिए इस्तेमाल होने वाली अनएन्क्रिप्टेड प्रॉक्सी रूटिंग प्रणाली।

चेकपॉइंट 5: क्रॉसवर्ड पहेली

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



बाएँ से दाएँ

2. आधुनिक, तेज़ और हल्का वीपीएन प्रोटोकॉल (5)

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

6. अलग-अलग जगहों पर फैले सर्वरों का जाल (7)

7. एन्क्रिप्टेड रास्ते से बना इंटरनेट संपर्क (8)

ऊपर से नीचे

1. वह शहर या देश जहाँ सर्वर स्थित है (5)

4. संचार जाल को हमलों और घुसपैठ से बचाने के उपाय (7)

5. जोखिम घटाने के लिए उठाए गए कदम (6)

6. सर्वर के माध्यम से मिलने वाली कनेक्शन की रफ़्तार (5)

चेकपॉइंट 5, वैकल्पिक: सुलभ क्रॉसवर्ड संकेत

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

बाएँ से दाएँ

2 बाएँ से दाएँ: आधुनिक, तेज़ और हल्का वीपीएन प्रोटोकॉल (5 अक्षर):

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

6 बाएँ से दाएँ: अलग-अलग जगहों पर फैले सर्वरों का जाल (7 अक्षर):

7 बाएँ से दाएँ: एन्क्रिप्टेड रास्ते से बना इंटरनेट संपर्क (8 अक्षर):

ऊपर से नीचे

1 ऊपर से नीचे: वह शहर या देश जहाँ सर्वर स्थित है (5 अक्षर):

4 ऊपर से नीचे: संचार जाल को हमलों और घुसपैठ से बचाने के उपाय (7 अक्षर):

5 ऊपर से नीचे: जोखिम घटाने के लिए उठाए गए कदम (6 अक्षर):

6 ऊपर से नीचे: सर्वर के माध्यम से मिलने वाली कनेक्शन की रफ़्तार (5 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।

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

शब्दावली शब्द-सूची

वायरगार्ड सर्वरगति सर्वरनेटवर्क सर्वरस्थान सुरक्षितकनेक्शन कनेक्शनगति नेटवर्कसुरक्षा सुरक्षाउपाय

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. सर्वरगति
C. सर्वरनेटवर्क
D. सर्वरस्थान
E. सुरक्षितकनेक्शन
F. कनेक्शनगति
G. नेटवर्कसुरक्षा
H. सुरक्षाउपाय

परिभाषाएँ और मिलान फ़ील्ड	
	1. सर्वर के माध्यम से मिलने वाली कनेक्शन की रफ़्तार।
	2. जोखिम घटाने के लिए उठाए गए कदम।
	3. वीपीएन चालू होने पर मिलने वाली इंटरनेट रफ़्तार।
	4. अलग-अलग जगहों पर फैले सर्वरों का जाल।
	5. आधुनिक, तेज़ और हल्का वीपीएन प्रोटोकॉल।
	6. संचार जाल को हमलों और घुसपैठ से बचाने के उपाय।
	7. वह शहर या देश जहाँ सर्वर स्थित है।
	8. एन्क्रिप्टेड रास्ते से बना इंटरनेट संपर्क।

चेकपॉइंट 7: उलझे शब्दों की चुनौती

नीचे के अक्षरों को सुलझाकर वर्चुअल प्राइवेट नेटवर्क (VPN) की प्रमुख अवधारणाएँ और शब्द पता करें। अपने उत्तर दिए गए इनपुट बॉक्स में लिखें।

1. गा र वा र्ड य
2. स र र्क व ट ने र्व
3. त र सु क ने न क्श क्षि
4. क्षा ट सु र्क र ने व
5. र ति स ग र्व
6. स्था स र न र्व
7. ग क न ति क्श ने
8. क्षा य सु पा उ र

अतिरिक्त गतिविधि: झटपट सोचें

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

1	एक अच्छे VPN ऐप का वर्णन करने वाले शब्द			
2	ऐसी चीज़ें जिन्हें IPVanish आपके नेटवर्क से छिपा सकता है			
3	ऐसी जगहें जहाँ आप IPVanish चालू करेंगे			
4	आपके जाने-पहचाने VPN प्रोटोकॉल			
5	IPVanish कस्टमर सपोर्ट के लिए सवाल			
6	ऐसे देश जहाँ आप IPVanish सर्वर चाहेंगे			
7	IPVanish के अलावा अन्य VPN सेवाएँ			
8	ऐसी स्थितियाँ जिनमें किल स्विच मददगार होता है			
9	IPVanish चुनने के कारण			
10	आपका VPN कनेक्शन धीमा होने के संकेत			
11	ऐसी चीज़ें जो आप रोज़ ऑनलाइन करते हैं			
12	ऐसे लोग जिन्हें आप IPVanish की सलाह देंगे			
13	VPN खरीदने से पहले जाँचने वाली चीज़ें			
14	इस वर्कशीट में आपके सीखे हुए सुरक्षा शब्द			
15	IPVanish में आप जिन सुविधाओं को देखते हैं			

चेकपॉइंट 8: VPN और नेटवर्क केस स्टडी

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

केस स्टडी 1: मीडिया सेंटर कॉन्फ़िगरेशन



परिदृश्य: एक ग्राहक तेज़ थ्रूपुट बनाए रखते हुए सुरक्षित रूप से स्ट्रीम करने के लिए IPVanish का उपयोग करके अपना Android Fire TV मीडिया प्लेयर सुरक्षित करना चाहता है।

चर्चा प्रश्न: संसाधन-सीमित स्ट्रीमिंग हार्डवेयर के लिए OpenVPN की तुलना में WireGuard प्रोटोकॉल को प्राथमिकता क्यों दी जाती है?

केस स्टडी 2: टोरेंट नेटवर्क प्रॉक्सी



परिदृश्य: एक P2P अपलोडर SOCKS5 कॉन्फ़िगरेशन का उपयोग करके पूर्ण डेटा एन्क्रिप्शन के ओवरहेड के बिना अपनी लोकेशन छिपाना चाहता है।

चर्चा प्रश्न: SOCKS5 प्रॉक्सी बनाम पूर्ण IPVanish VPN टनल के उपयोग के सुरक्षा और स्पीड संबंधी समझौतों की तुलना कीजिए।

चेकपॉइंट 9: कूट संदेश को डिकोड करें

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

अक्षर-से-संख्या एन्क्रिप्शन कुंजी

अ=1 आ=2 इ=3 ई=4 उ=5 ऊ=6 ऋ=7 ए=8 ऐ=9 ओ=10 औ=11 ऑ=12

क=13 ख=14 ग=15 घ=16 ङ=17 च=18 छ=19 ज=20 झ=21 ञ=22 ट=23 ठ=24

ड=25 ढ=26 ण=27 त=28 थ=29 द=30 ध=31 न=32 प=33 फ=34 ब=35 भ=36

म=37 य=38 र=39 ल=40 व=41 श=42 ष=43 स=44 ह=45 ा=46 ि=47 ी=48

ु=49 ू=50 ृ=51 े=52 ै=53 ो=54 ौ=55 ॉ=56 ं=57 ँ=58 ः=59 ़=60

्=61

2	4	33	48	41	53	32	47	42		44	14	61	28		32	54

40	56	15	61	44		26	46	58	18	46		1	33	32	46	28	46

डिकोड किया गया संदेश:

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

चेकपॉइंट 10: बुनियादी VPN FAQ (भाग A)

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

Q1: IPVanish में डिफ़ॉल्ट प्रोटोकॉल कौन-सा है?

यह डिफ़ॉल्ट रूप से उच्च गति वाले WireGuard से रूट करता है।

Q2: क्या IPVanish अपने सर्वर हार्डवेयर का मालिक है?

हाँ, यह अपने भौतिक सर्वर नेटवर्क के बड़े हिस्से का स्वामित्व रखता है और उसे स्वयं संचालित करता है।

Q3: IPVanish कहाँ स्थित है?

यह संयुक्त राज्य अमेरिका में स्थित है और अमेरिकी कानूनों के अधीन है।

Q4: एक साथ कितने डिवाइस कनेक्ट हो सकते हैं?

IPVanish प्रति खाता असीमित एक साथ डिवाइस कनेक्शन देता है।

Q5: क्या यह कोई कनेक्शन लॉग रखता है?

नहीं, यह सख़्त ज़ीरो-लॉग्स नीति लागू करता है, जिसे स्वतंत्र ऑडिट ने मान्य किया है। [6]

चेकपॉइंट 10: बुनियादी VPN FAQ (भाग B)

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

Q6: क्या IPVanish प्रॉक्सी सेवा देता है?

हाँ, यह टॉरेंटिंग के लिए मुफ़्त SOCKS5 प्रॉक्सी देता है।

Q7: क्या इसमें किल स्विच शामिल है?

हाँ, किल स्विच Windows, macOS, Android और iOS पर उपलब्ध है।

Q8: क्या मैं IPVanish से जियो-ब्लॉक बायपास कर सकता हूँ?

हाँ, इसके सर्वरों का वैश्विक नेटवर्क प्रतिबंधित लाइब्रेरी तक पहुँच देता है।

Q9: क्या यह स्प्लिट टनलिंग सपोर्ट करता है?

हाँ, स्प्लिट टनलिंग उपलब्ध है, जिसमें Windows और Android भी शामिल हैं।

Q10: यह कौन-से एन्क्रिप्शन सिफ़र का उपयोग करता है?

यह AES-256 और ChaCha20 एन्क्रिप्शन का उपयोग करके कनेक्शन सुरक्षित करता है।

चेकपॉइंट 10: उन्नत VPN FAQ (भाग C)

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

Q1: SOCKS5 प्रॉक्सी कैसे कॉन्फ़िगर की जाती है?

इसे टोरेंट क्लाइंट में एन्क्रिप्शन ओवरहेड के बिना उपयोगकर्ता का IP छिपाने के लिए सेट किया जाता है।

Q2: सर्वर हार्डवेयर का मालिक होना सुरक्षा कैसे बढ़ाता है?

यह तृतीय-पक्ष सर्वर किराये पर लेने के जोखिम घटाता है और प्रदाता को सर्वर कॉन्फ़िगरेशन पर सीधा नियंत्रण देता है।

Q3: US के अधिकार क्षेत्र का गोपनीयता पर क्या प्रभाव पड़ता है?

हालाँकि अमेरिकी कानून डेटा प्रतिधारण अनिवार्य नहीं करते, वे नेशनल सिक्योरिटी लेटर और वारंट की अनुमति देते हैं।

Q4: किल स्विच IP लीक कैसे रोकता है?

VPN कनेक्शन अचानक टूटने पर यह सभी इंटरनेट एडॉप्टर ब्लॉक कर देता है।

Q5: WireGuard के साथ कौन-सा एन्क्रिप्शन उपयोग होता है?

WireGuard ChaCha20 सिमेट्रिक कुंजी एन्क्रिप्शन और Poly1305 प्रमाणीकरण का उपयोग करता है। [7]

चेकपॉइंट 10: उन्नत VPN FAQ (भाग D)

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

Q6: ज़ीरो-लॉग्स नीति कैसे सत्यापित की जाती है?

Leviathan Security Group ने 2022 में और Schellman ने 2025 में इसका ऑडिट किया; किसी को भी उपयोगकर्ता लॉग नहीं मिले। [3]

Q7: यह IPv6 DNS क्वेरी कैसे संभालता है?

यह सभी DNS और IPv6 क्वेरी को अपने निजी नेमसर्वर से अपने-आप रूट करता है।

Q8: क्या IPVanish ऑब्फ़स्केशन सुविधाएँ देता है?

हाँ, इसका Scramble फ़ीचर फ़ायरवॉल को बायपास करने के लिए OpenVPN ट्रैफ़िक को ऑब्फ़स्केट करता है।

Q9: मोबाइल डिवाइस पर स्प्लिट टनलिंग कैसे काम करती है?

यह चुने हुए ऐप्स को VPN टनल बायपास करके सीधे कनेक्ट होने देता है।

Q10: क्या यह राउटर कॉन्फ़िगरेशन को सपोर्ट करता है?

हाँ, OpenVPN और WireGuard कॉन्फ़िगरेशन DD-WRT राउटरों पर मैन्युअल रूप से लोड किए जा सकते हैं। [1]

भाग 11: 10 वास्तविक VPN तथ्य और अंतर्दृष्टियाँ

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

1. VPN इनसाइट

IPVanish अपने अधिकांश सर्वर इन्फ्रास्ट्रक्चर का मालिक है, उसे तृतीय पक्षों से किराये पर नहीं लेता। [3]

2. VPN इनसाइट

IPVanish 2012 से संचालित है और इसका स्वामित्व Ziff Davis के पास है, जिसे पहले J2 Global के नाम से जाना जाता था। [2]

3. VPN इनसाइट

SOCKS5 प्रॉक्सी क्लाइंट का सार्वजनिक IP पता छिपाता है, लेकिन डेटा पैकेट एन्क्रिप्ट नहीं करता।

4. VPN इनसाइट

WireGuard डिफ़ॉल्ट प्रोटोकॉल है, और ऐप्स में OpenVPN तथा IKEv2/IPSec भी उपलब्ध हैं। [2]

5. VPN इनसाइट

मानक OpenVPN Scramble फ़ायरवॉल को बायपास करने के लिए पैकेट हेडर पर XOR ऑब्फ़स्केशन परत जोड़ता है।

6. VPN इनसाइट

असीमित समवर्ती कनेक्शन नीति उपयोगकर्ताओं को अपने घर के सभी डिवाइस एक साथ सुरक्षित करने देती है। [2]

7. VPN इनसाइट

Leviathan Security Group (2022) और Schellman (2025) के ऑडिट ने इसके नो-लॉग्स दावों की पुष्टि की। [3]

8. VPN इनसाइट

Android ऐप ऑलवेज़-ऑन VPN सेटिंग्स को सपोर्ट करता है, जो टनल डिस्कनेक्ट होने पर इंटरनेट एक्सेस रोक देती हैं।

9. VPN इनसाइट

OpenVPN कनेक्शन गति के लिए UDP या फ़ायरवॉल के पार स्थिर रूटिंग के लिए TCP, दोनों में से कोई भी इस्तेमाल कर सकते हैं।

10. VPN इनसाइट

यह 24/7 लाइव चैट सपोर्ट देता है, साथ ही तय कार्यदिवस के व्यावसायिक घंटों में फ़ोन सपोर्ट भी देता है। [5]

तकनीकी संदर्भ और स्रोत

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

शैक्षणिक और उद्योग संदर्भ

[1] VPN.com. (2026). IPVanish Review.
https://www.vpn.com/vpn/ipvanish/

[2] Security.org. (2026). IPVanish VPN Review 2026.
https://www.security.org/vpn/ipvanish/review/

[3] All Things VPN. (2026). IPVanish Review 2026: Speeds, Streaming, & Privacy Tested.
https://allthingsvpn.com/ipvanish-review/

[4] Cloudwards. (2026). IPVanish Review 2026 [VPN Features, Pricing & Speed].
https://www.cloudwards.net/ipvanish-review/

[5] Top10VPN. (2026). IPVanish Review: Surprising Results from a Dark Horse.
https://www.top10vpn.com/reviews/ipvanish/

[6] IPVanish, Inc. (n.d.). IPVanish VPN: Fast & Secure [App Store listing].
https://apps.apple.com/us/app/ipvanish-vpn-fast-secure/id763638165

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

[8] Leech, M., et al. (1996). RFC 1928: SOCKS Protocol Version 5. IETF.
https://www.rfc-editor.org/rfc/rfc1928

[9] Nir, Y., & Langley, A. (2018). RFC 8439: ChaCha20 and Poly1305 for IETF Protocols. IETF.
https://www.rfc-editor.org/rfc/rfc8439

[10] Android Developers. (n.d.). VPN.
https://developer.android.com/develop/connectivity/vpn

उत्तर कुंजी: चेकपॉइंट 1 – बहुविकल्पीय

1 **WireGuard डिफ़ॉल्ट** WIREGUARD **सही उत्तर: A**

शिक्षण नोट

WireGuard अनुकूलित रूटिंग गति के लिए डिफ़ॉल्ट रूप से कॉन्फ़िगर है। उद्धरण: IPVanish Features।

2 **SOCKS5 प्रॉक्सी** SOCKS5 प्रॉक्सी **सही उत्तर: A**

शिक्षण नोट

SOCKS5 प्रॉक्सी एन्क्रिप्शन के ओवरहेड के बिना क्लाइंट की लोकेशन छिपाते हैं। उद्धरण: IPVanish Support।

3 **प्रश्न 3** **सही उत्तर: A**

शिक्षण नोट

Leviathan Security Group ने 2022 में IPVanish का पहला नो-लॉग्स ऑडिट किया; 2025 में Schellman ने किया। [3]

4 **अमेरिकी क्षेत्राधिकार** संयुक्त राज्य अमेरिका **सही उत्तर: A**

शिक्षण नोट

IPVanish संयुक्त राज्य अमेरिका में स्थित है, जो Five Eyes गठबंधन के नियमों के अधीन है। उद्धरण: IPVanish Review।

5 **असीमित डिवाइस** असीमित **सही उत्तर: A**

शिक्षण नोट

IPVanish असीमित एक साथ डिवाइस कनेक्शन की अनुमति देता है। उद्धरण: IPVanish Support।

उत्तर कुंजी: चेकपॉइंट 2 – सही या गलत

6 **सर्वर हार्डवेयर** OWNS NETWORK — **सही उत्तर: सही**

शिक्षण नोट

IPVanish अपने भौतिक सर्वर नेटवर्क के बड़े हिस्से का मालिक है और उसका प्रबंधन करता है। उद्धरण: IPVanish Support।

7 **प्रश्न 7** — **सही उत्तर: गलत**

शिक्षण नोट

गलत: SOCKS5 प्रॉक्सी आपका IP एड्रेस छिपाती है, लेकिन डेटा को एन्क्रिप्ट नहीं करती।

8 **प्रश्न 8** — **सही उत्तर: गलत**

शिक्षण नोट

गलत: IPVanish अपने डेस्कटॉप और मोबाइल ऐप्स में किल स्विच देता है।

9 **अमेरिकी क्षेत्राधिकार** फ़ाइव आइज़ US — **सही उत्तर: सही**

शिक्षण नोट

IPVanish अमेरिका में स्थित है, जो Five Eyes निगरानी नियमों के अधीन है। उद्धरण: IPVanish Review।

10 **स्प्लिट टनल** स्प्लिट रूट — **सही उत्तर: सही**

शिक्षण नोट

स्प्लिट टनलिंग विशिष्ट ऐप का ट्रैफ़िक सुरक्षित टनल के बाहर रूट करती है। उद्धरण: IPVanish Support।

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. WireGuard	H 2. SOCKS5 प्रॉक्सी	D 3. सर्वर स्पीड	A 4. Kill Switch
G 5. ऑडिट किए गए लॉग	C 6. डिवाइस सीमा	E 7. IP पता	F 8. सुरक्षा

चेकपॉइंट 3: उत्तर – प्रमुख शब्द

1 वायरगार्ड	2 SOCKS5 प्रॉक्सी	3 सर्वर गति	4 सर्वर स्थान
5 सुरक्षित कनेक्शन	6 कनेक्शन गति		

चेकपॉइंट 6, वैकल्पिक: उत्तर – शब्द मिलान

1 B – सर्वरगति	2 H – सुरक्षाउपाय	3 F – कनेक्शनगति	4 C – सर्वरनेटवर्क
5 A – वायरगार्ड	6 G – नेटवर्कसुरक्षा	7 D – सर्वरस्थान	8 E – सुरक्षितकनेक्शन

शिक्षकों के लिए चर्चा नोट

प्रमुख शब्द:
जाँचें कि क्या विद्यार्थी WireGuard, SOCKS5 प्रॉक्सी और सर्वर स्पीड 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

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

क्रॉसवर्ड समाधान



क्रॉसवर्ड समाधान के लिए शिक्षक गाइड

बाएँ से दाएँ

2 बाएँ से दाएँ: वायरगार्ड आधुनिक, तेज़ और हल्का वीपीएन प्रोटोकॉल (5 अक्षर)

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

6 बाएँ से दाएँ: सर्वरनेटवर्क अलग-अलग जगहों पर फैले सर्वरों का जाल (7 अक्षर)

7 बाएँ से दाएँ: सुरक्षितकनेक्शन एन्क्रिप्टेड रास्ते से बना इंटरनेट संपर्क (8 अक्षर)

ऊपर से नीचे

1 ऊपर से नीचे: सर्वरस्थान वह शहर या देश जहाँ सर्वर स्थित है (5 अक्षर)

4 ऊपर से नीचे: नेटवर्कसुरक्षा संचार जाल को हमलों और घुसपैठ से बचाने के उपाय (7 अक्षर)

5 ऊपर से नीचे: सुरक्षाउपाय जोखिम घटाने के लिए उठाए गए कदम (6 अक्षर)

6 ऊपर से नीचे: सर्वरगति सर्वर के माध्यम से मिलने वाली कनेक्शन की रफ़्तार (5 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. सरर्कवटनेर्व — **सर्वरनेटवर्क**
3. तरसुकनेनक्षक्षि — **सुरक्षितकनेक्शन**
4. क्षाटसुर्करनेव — **नेटवर्कसुरक्षा**
5. रतिसगर्व — **सर्वरगति**
6. स्थासरनर्व — **सर्वरस्थान**
7. गकनतिक्शने — **कनेक्शनगति**
8. क्षायसुपाउर — **सुरक्षाउपाय**

गुप्त कूट चुनौती कुंजी

"आईपीवैनिश सख्त नो लॉग्स ढाँचा अपनाता"

केस स्टडी के उत्तर

A केस स्टडी 1: मीडिया सेंटर कॉन्फ़िगरेशन

शिक्षक समाधान

ग्रेडिंग दिशानिर्देश

छात्रों के उत्तरों में निम्नलिखित बिंदु शामिल होने चाहिए:

- परिदृश्य विश्लेषण: एक क्लाइंट तेज़ थ्रूपुट बनाए रखते हुए सुरक्षित स्ट्रीमिंग के लिए IPVanish से अपना Android Fire TV मीडिया प्लेयर सुरक्षित करना चाहता है।
- अनुशंसित रणनीति और समाधान: मूल्यांकन मार्गदर्शन: समझाएँ कि WireGuard का कोड छोटा है, वह कर्नेल स्पेस के भीतर चलता है और कम CPU साइकल इस्तेमाल करता है, जिससे हल्के हार्डवेयर पर गति अधिकतम होती है।

B केस स्टडी 2: टोरेंट नेटवर्क प्रॉक्सी

शिक्षक समाधान

ग्रेडिंग दिशानिर्देश

छात्रों के उत्तरों में निम्नलिखित बिंदु शामिल होने चाहिए:

- परिदृश्य विश्लेषण: एक P2P अपलोडर SOCKS5 कॉन्फ़िगरेशन से, पूरे डेटा एन्क्रिप्शन के ओवरहेड के बिना, अपनी लोकेशन छिपाना चाहता है।
- अनुशंसित रणनीति और समाधान: मूल्यांकन मार्गदर्शन: ध्यान दें कि SOCKS5 ट्रैफ़िक को एन्क्रिप्ट किए बिना IP पता छिपाता है, जिससे गति तेज़ मिलती है लेकिन ISP की पैकेट जाँच के विरुद्ध कोई गोपनीयता नहीं रहती।