नाम: _____ दिनांक: _____ अंक: _____

CyberGhost सुरक्षा

CyberGhost के सुरक्षा इन्फ्रास्ट्रक्चर, रोमानिया में उसके स्वामित्व वाले NoSpy सर्वर ऐरे, डिस्कलेस केवल-RAM सर्वर नोड, AES-256 एन्क्रिप्शन और स्वचालित kill switch सुरक्षा का मूल्यांकन।

CyberGhost सुरक्षा 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 CyberGhost की सुरक्षा सुविधाओं से परिचित कराता है। आप स्वयं के स्वामित्व वाले NoSpy सर्वर समूह, डिस्कलेस RAM-only हार्डवेयर, सिफ़र और किल स्विच 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/cyberghost/suraksha/

आपका CyberGhost सुरक्षा लर्निंग रोडमैप

- CyberGhost Security की तकनीकी संरचना और कॉन्फ़िगरेशन नियमों का विश्लेषण करें।
- IP, DNS और WebRTC ट्रैफ़िक लीक रोकने के लिए क्लाइंट सेटिंग्स कॉन्फ़िगर करें।
- कस्टम मूल्य निर्धारण, ट्रायल और प्रदर्शन सुविधाओं की तुलना मानक मॉडलों से करें।

CyberGhost सुरक्षा गाइड 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 एन्क्रिप्शन और NoSpy सर्वर पर लागू करें। अंत में अतिरिक्त गतिविधि झटपट सोचें पूरी करें।

स्वामित्व वाले NoSpy सर्वर इंफ़्रास्ट्रक्चर और डिस्कलेस नोड (परिचय)

CyberGhost बुखारेस्ट, रोमानिया स्थित अपने मुख्यालय से निजी रूप से प्रबंधित NoSpy सर्वर चलाता है, जिससे व्यावसायिक होस्ट के जोखिम बायपास हो जाते हैं। सुरक्षा AES-256 सिफ़र, डिस्कलेस RAM-only हार्डवेयर और स्वचालित किल स्विच से लागू की जाती है।

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

चेकपॉइंट 1: बहुविकल्पीय चुनौती

1. CyberGhost सभी प्रमुख प्लेटफ़ॉर्म पर कौन-सा प्रोटोकॉल देता है?
   - A) WireGuard
   - B) OpenVPN
   - C) IKEv2
   - D) L2TP

2. CyberGhost के OpenVPN और IKEv2 कनेक्शन कौन-सा सिफ़र इस्तेमाल करते हैं?
   - A) AES-256
   - B) Blowfish-128
   - C) DES-56
   - D) RC4

3. CyberGhost के स्वयं संचालित NoSpy सर्वर कहाँ स्थित हैं?
   - A) रोमानिया
   - B) जर्मनी
   - C) संयुक्त राज्य अमेरिका
   - D) स्विट्ज़रलैंड

4. कौन-सा इंफ्रास्ट्रक्चर प्रकार पावर बंद होने पर डिस्क पर शून्य लॉग रखता है?
   - A) केवल RAM वाले सर्वर
   - B) HDD सर्वर
   - C) वर्चुअल सर्वर
   - D) हाइब्रिड सर्वर

5. VPN के बीच में कटने पर कौन-सी सुविधा कनेक्शन ब्लॉक करती है?
   - A) Kill Switch
   - B) स्प्लिट टनलिंग
   - C) Smart DNS
   - D) पोर्ट फ़ॉरवर्ड

चेकपॉइंट 2: सही या गलत चुनौती

6 प्रश्न 6

6. CyberGhost का मुख्यालय रोमानिया में है, जो 14-Eyes समूह से बाहर है।

○ सही ○ गलत

7 प्रश्न 7

7. NoSpy सर्वर थर्ड-पार्टी व्यावसायिक डेटासेंटर से किराये पर लिए जाते हैं।

○ सही ○ गलत

8 प्रश्न 8

8. RAM-only सर्वर उपयोगकर्ता सेशन डेटा को स्थायी सॉलिड-स्टेट ड्राइव पर लिखते हैं।

○ सही ○ गलत

9 प्रश्न 9

9. क्लाइंट ऐप में DNS लीक से अंतर्निहित सुरक्षा है।

○ सही ○ गलत

10 प्रश्न 10

10. CyberGhost की ज़ीरो-लॉग्स नीति स्वतंत्र ऑडिट द्वारा सत्यापित की गई 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. मोबाइल कनेक्शन के लिए अनुशंसित उच्च प्रदर्शन वाला प्रोटोकॉल _____ है।

2. मज़बूत एन्क्रिप्शन और कई परतों वाला _____ मिलकर आपका पेलोड ट्रैफ़िक सुरक्षित रखते हैं।

3. कंपनी की कठोर _____ के तहत उपयोगकर्ताओं की गतिविधि के लॉग रखे ही नहीं जाते।

4. कंपनी अपने ही नियंत्रण में रखे गए उच्च-सुरक्षा _____ चलाती है, जिन्हें किसी तीसरे पक्ष को नहीं सौंपा जाता।

5. बिजली बंद होने के बाद डेटा बचा न रहे, इसके लिए वे _____ डिस्क-रहित ढांचे इस्तेमाल करते हैं।

6. कनेक्शन टूटने पर असुरक्षित ट्रैफ़िक उजागर होने से _____ फेल-सेफ़ स्विच रोकता है।

शब्दावली शब्द-बैंक

किल स्विच | केवल रैम | रोमानिया | वायरगार्ड | सुरक्षा कवच | सुरक्षा नीति | सुरक्षित सर्वर | AES-256

अपने उत्तर यहाँ लिखें:

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

चेकपॉइंट 4: VPN और नेटवर्क अवधारणा मिलान

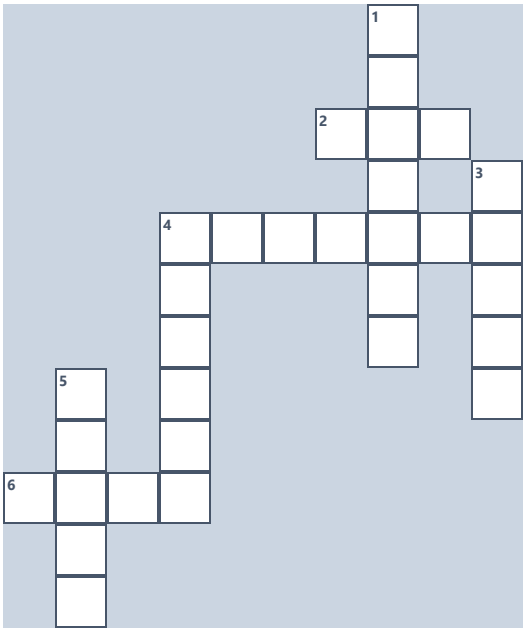
परिभाषा मिलान

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**	14-Eyes गठबंधनों से बाहर स्थित राष्ट्रीय गोपनीयता क्षेत्राधिकार।
☐	**2. AES-256**	**B**	डिस्कलेस सर्वर इन्फ्रास्ट्रक्चर जो कोई स्थायी लॉग नहीं लिखता।
☐	**3. रोमानिया**	**C**	रिज़ॉल्वर अनुरोधों का VPN के बाहर अनजाने में उजागर होना।
☐	**4. NoSpy**	**D**	CyberGhost ऐप्स में उपलब्ध तेज़ स्पीड वाला ओपन-सोर्स प्रोटोकॉल।
☐	**5. केवल-RAM**	**E**	थर्ड-पार्टी सत्यापन, जो ज़ीरो-लॉग्स अनुपालन के दावों की समीक्षा करता है।
☐	**6. KILL SWITCH**	**F**	टनल से गुज़रने वाले पेलोड को सुरक्षित करने वाला सिमेट्रिक सिफ़र मानक।
☐	**7. लीक**	**G**	रोमानिया में संचालित पूरी तरह स्वामित्व वाला उच्च-सुरक्षा सर्वर समूह।
☐	**8. ऑडिट**	**H**	फ़ेलसेफ़ क्लाइंट यूटिलिटी जो ड्रॉप होने पर इंटरनेट ट्रैफ़िक काट देती है।

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. आपके डिवाइस और सर्वर के बीच बना एन्क्रिप्टेड निजी रास्ता (3)

4. ऐसा सर्वर, जिस तक अनधिकृत पहुंच रोकने के उपाय किए गए हों (7)

6. कनेक्शन टूटने पर इंटरनेट ट्रैफ़िक काट देने वाली फेल-सेफ़ क्लाइंट यूटिलिटी (4)

ऊपर से नीचे

1. VPN के बाहर रिज़ॉल्वर अनुरोधों का अनचाहा उजागर होना (7)

3. सुरक्षा के नियमों और कदमों का लिखित ढांचा (5)

4. डेटा और उपकरणों को हमलों से बचाने वाली सुरक्षा की परत (6)

5. डिस्क-रहित सर्वर ढांचा, जो कोई स्थायी लॉग नहीं लिखता (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: आपके डिवाइस और सर्वर के बीच बना एन्क्रिप्टेड निजी रास्ता (3 अक्षर):

4 बाएँ से दाएँ: ऐसा सर्वर, जिस तक अनधिकृत पहुंच रोकने के उपाय किए गए हों (7 अक्षर):

6 बाएँ से दाएँ: कनेक्शन टूटने पर इंटरनेट ट्रैफ़िक काट देने वाली फेल-सेफ़ क्लाइंट यूटिलिटी (4 अक्षर):

ऊपर से नीचे

1 ऊपर से नीचे: VPN के बाहर रिज़ॉल्वर अनुरोधों का अनचाहा उजागर होना (7 अक्षर):

3 ऊपर से नीचे: सुरक्षा के नियमों और कदमों का लिखित ढांचा (5 अक्षर):

4 ऊपर से नीचे: डेटा और उपकरणों को हमलों से बचाने वाली सुरक्षा की परत (6 अक्षर):

5 ऊपर से नीचे: डिस्क-रहित सर्वर ढांचा, जो कोई स्थायी लॉग नहीं लिखता (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।

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

शब्दावली शब्द-सूची

सुरक्षानीति, डीएनएसलीक, सुरक्षाकवच, वायरगार्ड, टनल, केवलरैम, किलस्विच, सुरक्षितसर्वर

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. सुरक्षानीति
B. डीएनएसलीक
C. सुरक्षाकवच
D. वायरगार्ड
E. टनल
F. केवलरैम
G. किलस्विच
H. सुरक्षितसर्वर

परिभाषाएँ और मिलान फ़ील्ड
1. कनेक्शन टूटने पर इंटरनेट ट्रैफ़िक काट देने वाली फेल-सेफ़ क्लाइंट यूटिलिटी।
2. सुरक्षा के नियमों और कदमों का लिखित ढांचा।
3. CyberGhost के सभी ऐप्स में उपलब्ध तेज़, ओपन-सोर्स प्रोटोकॉल।
4. डिस्क-रहित सर्वर ढांचा, जो कोई स्थायी लॉग नहीं लिखता।
5. VPN के बाहर रिज़ॉल्वर अनुरोधों का अनचाहा उजागर होना।
6. डेटा और उपकरणों को हमलों से बचाने वाली सुरक्षा की परत।
7. ऐसा सर्वर, जिस तक अनधिकृत पहुंच रोकने के उपाय किए गए हों।
8. आपके डिवाइस और सर्वर के बीच बना एन्क्रिप्टेड निजी रास्ता।

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. **नी क्षा सु ति र** _____

2. **च सु क्षा व क र** _____

3. **ल न ट** _____

4. **च स्वि कि ल** _____

5. **स क ए न डी ली ए** _____

6. **गा वा र र्ड य** _____

7. **रै म के ल व** _____

8. **र त र सु र्व स क्षि** _____

अतिरिक्त गतिविधि: झटपट सोचें

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

1	स्ट्रीमिंग सेवाएँ जो आप देखते हैं			
2	VPN ऐप के बटन या मेनू			
3	अतिरिक्त सुरक्षा के लिए आप जो सेटिंग्स चालू करते हैं			
4	CyberGhost के अलावा अन्य VPN सेवाएँ			
5	ऐसी चीज़ें जिन्हें एन्क्रिप्शन सुरक्षित रखता है			
6	ऐसी चीज़ें जिन्हें CyberGhost आपके नेटवर्क से छिपा सकता है			
7	सार्वजनिक Wi-Fi पर खतरे			
8	VPN लीक के प्रकार			
9	CyberGhost की सुरक्षा सुविधाएँ			
10	ऐसी चीज़ें जिन्हें ऑडिट जाँच सकता है			
11	ऐसी स्थितियाँ जिनमें किल स्विच मददगार होता है			
12	मज़बूत गोपनीयता कानूनों के लिए जाने जाने वाले देश			
13	एक अच्छे VPN ऐप का वर्णन करने वाले शब्द			
14	ऐसे देश जहाँ आप CyberGhost सर्वर चाहेंगे			
15	मज़बूत पासवर्ड बनाने के तरीके			

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: अधिकार क्षेत्र के आधार पर गोपनीयता ऑडिट



परिदृश्य: एक मीडिया कंपनी यह सुनिश्चित करना चाहती है कि कॉर्पोरेट खुफ़िया रिकॉर्ड विदेशी कानून प्रवर्तन द्वारा सम्मन के ज़रिए न माँगे जा सकें।

चर्चा प्रश्न: CyberGhost का रोमानियाई मुख्यालय कंपनी को निगरानी वारंटों से कैसे बचाता है?

केस स्टडी 2: हार्डवेयर ज़ब्ती से सुरक्षा



परिदृश्य: एक सर्वर सुविधा में अनधिकृत भौतिक घुसपैठ होती है और VPN सर्वर रैक ज़ब्त कर लिया जाता है।

चर्चा प्रश्न: कौन-सा हार्डवेयर डिज़ाइन घुसपैठियों को सेशन कुंजियाँ या उपयोगकर्ता इतिहास निकालने से रोकता है?

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

32	54	44	61	33	46	4		44	39	61	41	39		1	31	47	13	28	37

25	52	23	46		15	54	33	32	48	38	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: क्या CyberGhost सुरक्षित है?

हाँ, यह AES-256 एन्क्रिप्शन, सुरक्षित प्रोटोकॉल का उपयोग करता है और रोमानिया के गोपनीयता कानूनों के तहत संचालित होता है।

Q2: NoSpy सर्वर क्या हैं?

अधिकतम सुरक्षा के लिए NoSpy सर्वर केवल CyberGhost द्वारा अपने रोमानियाई मुख्यालय में स्वामित्व में रखे, बनाए और प्रबंधित किए जाते हैं।

Q3: क्या CyberGhost लॉग रखता है?

नहीं, यह सख़्त ज़ीरो-लॉग्स नीति लागू करता है, यानी कोई ब्राउज़िंग इतिहास या कनेक्शन लॉग संग्रहीत नहीं होता।

Q4: CyberGhost कहाँ स्थित है?

CyberGhost का मुख्यालय बुखारेस्ट, रोमानिया में है, जहाँ की संवैधानिक अदालत ने 2009 और 2014 में व्यापक डेटा प्रतिधारण कानूनों को रद्द कर दिया था, हालाँकि 2015 का एक कानून इलेक्ट्रॉनिक संचार प्रदाताओं से फिर कुछ ट्रैफ़िक डेटा रखने की अपेक्षा करता है।

Q5: यह कौन-से प्रोटोकॉल उपयोग करता है?

यह डिवाइस के प्रकार के अनुसार WireGuard, OpenVPN (TCP/UDP) और IKEv2 प्रोटोकॉल को सपोर्ट करता है।

चेकपॉइंट 10: बुनियादी VPN FAQ (भाग B)

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

Q6: क्या यह विज्ञापन ब्लॉक करता है?

हाँ, क्लाइंट ऐप में विज्ञापन, ट्रैकिंग स्क्रिप्ट और मैलवेयर डोमेन के लिए बिल्ट-इन कंटेंट ब्लॉकर है।

Q7: क्या किल स्विच है?

हाँ, इसमें एक स्वचालित किल स्विच है जो VPN कनेक्शन टूटने पर इंटरनेट पहुँच ब्लॉक कर देता है।

Q8: क्या CyberGhost लीक से सुरक्षा देता है?

हाँ, ऐप्स में बिल्ट-इन DNS और IP लीक सुरक्षा है जो आपका असली IP छिपाती है।

Q9: क्या सर्वरों का ऑडिट होता है?

हाँ, CyberGhost की ज़ीरो-लॉग नीति और इंफ्रास्ट्रक्चर का Deloitte द्वारा स्वतंत्र रूप से ऑडिट किया गया है। [2]

Q10: क्या यह RAM सर्वरों का उपयोग करता है?

हाँ, CyberGhost के अनुसार उसका सर्वर नेटवर्क डिस्क-रहित, केवल-RAM हार्डवेयर पर चलता है।

चेकपॉइंट 10: उन्नत VPN FAQ (भाग C)

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

Q1: डिफ़ॉल्ट रूप से कौन-सा प्रोटोकॉल इस्तेमाल होता है?

ऐप सबसे अच्छा प्रोटोकॉल अपने-आप चुन लेता है, लेकिन आप कभी भी बदल सकते हैं।

Q2: स्प्लिट टनलिंग कैसे काम करती है?

यह आपको चुनने देता है कि कौन-से ऐप और वेबसाइट VPN का उपयोग करें और कौन-से टनल को बायपास करें।

Q3: DNS क्वेरी कहाँ जाती हैं?

इन्हें VPN टनल से CyberGhost के अपने DNS सर्वरों पर भेजा जाता है, आपके ISP के पास नहीं।

Q4: CyberGhost का स्वामी कौन है?

CyberGhost का स्वामित्व Kape Technologies के पास है, जिसके पास ExpressVPN और Private Internet Access का भी स्वामित्व है। [7]

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

WireGuard आधुनिक ChaCha20-Poly1305 सिमेट्रिक सिफ़र मानक का उपयोग करता है। [9]

चेकपॉइंट 10: उन्नत VPN FAQ (भाग D)

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

Q6: NoSpy सर्वर कैसे अलग हैं?

इनमें अधिक बैंडविड्थ वाला हार्डवेयर, समर्पित अपलिंक होते हैं और ये निजी डेटासेंटर में स्थित हैं।

Q7: क्या Dedicated IP गुमनाम होते हैं?

हाँ, IP को आपके खाते के बजाय एक रैंडम टोकन से जोड़ा जाता है, और टोकन हटा दिया जाता है।

Q8: नो-लॉग्स नीति का ऑडिट कौन करता है?

Deloitte Audit Romania, जिसने 2025 में CyberGhost का तीसरा नो-लॉग्स ऑडिट पूरा किया।

Q9: क्या ऐड ब्लॉकर HTTPS को डिक्रिप्ट करता है?

नहीं, विज्ञापन ब्लॉकर DNS स्तर पर काम करता है और विज्ञापन डोमेन को ब्लैक होल की ओर रिज़ॉल्व कर देता है।

Q10: क्या मैं राउटर पर CyberGhost इस्तेमाल कर सकता हूँ?

हाँ, घर के हर डिवाइस को कवर करने के लिए CyberGhost को VPN-संगत राउटर पर सेट करें।

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

CyberGhost का मुख्यालय रोमानिया में है, जो Five Eyes खुफ़िया-साझाकरण गठबंधन से बाहर है। [1]

2. VPN इनसाइट

OpenVPN और IKEv2 AES-256 का उपयोग करते हैं, जबकि WireGuard ChaCha20-Poly1305 का उपयोग करता है। [5]

3. VPN इनसाइट

NoSpy सर्वर CyberGhost के कर्मचारियों द्वारा आंतरिक रूप से स्वामित्व में रखे और प्रबंधित किए जाते हैं। [3]

4. VPN इनसाइट

Deloitte नियमित रूप से उनकी ज़ीरो-लॉग्स संचालन नीतियों का ऑडिट और सत्यापन करता है। [2]

5. VPN इनसाइट

डिस्कलेस, केवल-RAM सर्वर ऐसे पावर बंद होने पर डेटा को बने रहने से रोकते हैं। [1]

6. VPN इनसाइट

क्लाइंट ऐप में VPN कनेक्शन टूटने के लिए स्वचालित kill switch है।

7. VPN इनसाइट

बिल्ट-इन DNS और IP लीक सुरक्षा आपका असली IP छिपाए रखने में मदद करती है।

8. VPN इनसाइट

WireGuard, OpenVPN और IKEv2 प्रोटोकॉल क्लाइंट में मूल रूप से समर्थित हैं। [4]

9. VPN इनसाइट

डेडिकेटेड IP पते एक सुरक्षित, ज़ीरो-नॉलेज टोकन प्रणाली से दिए जाते हैं। [8]

10. VPN इनसाइट

बिल्ट-इन मैलवेयर फ़िल्टर दुर्भावनापूर्ण लक्ष्यों को ब्लॉक करने के लिए डोमेन लुकअप स्कैन करते हैं। [6]

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] CyberGhost VPN. (n.d.). No-Logs VPN: Secure & Private VPN with Zero Tracking.
https://www.cyberghostvpn.com/features/no-logs-vpn

[2] CyberGhost VPN. (2025). Third Deloitte Romania Audit Verifies Our Commitment to Privacy.
https://www.cyberghostvpn.com/privacyhub/privacy-audit-2025/

[3] CyberGhost VPN. (n.d.). CyberGhost's NoSpyServers: Complete Privacy & Anonymity.
https://www.cyberghostvpn.com/features/nospy

[4] CyberGhost VPN Support Center. (n.d.). Which VPN Protocols Do You Support?
https://support.cyberghostvpn.com/hc/en-us/articles/213983829-Which-VPN-Protocols-Do-You-Support

[5] CyberGhost VPN. (n.d.). VPN Encryption: How VPNs Help Secure Your Browsing.
https://www.cyberghostvpn.com/features/vpn-encryption

[6] CyberGhost VPN. (n.d.). VPN Features and Use Cases.
https://www.cyberghostvpn.com/features

[7] Kape Technologies. (n.d.). Our Brands.
https://www.kape.com/our-brands/

[8] CyberGhost VPN. (n.d.). Dedicated IP VPN | Get a Secure Static IP Address.
https://www.cyberghostvpn.com/dedicated-ip-vpn

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

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

[11] National Institute of Standards and Technology. (n.d.). FIPS 197: Advanced Encryption Standard (AES).
https://csrc.nist.gov/pubs/fips/197/final

[12] European Digital Rights (EDRi). (2014). Romania: The aftermath of the second CCR data retention ruling.
https://edri.org/our-work/romania-aftermath-of-second-ccr-data-retention-ruling/

उत्तर कुंजी: चेकपॉइंट 1 – बहुविकल्पीय

1 प्रश्न 1 — **सही उत्तर: A**

शिक्षण नोट

CyberGhost सभी प्रमुख प्लेटफ़ॉर्म पर कौन-सा प्रोटोकॉल देता है? → A) WireGuard

2 प्रश्न 2 — **सही उत्तर: A**

शिक्षण नोट

CyberGhost के OpenVPN और IKEv2 कनेक्शन कौन-सा सिफ़र इस्तेमाल करते हैं? → A) AES-256

3 प्रश्न 3 — **सही उत्तर: A**

शिक्षण नोट

CyberGhost के स्वयं संचालित NoSpy सर्वर कहाँ स्थित हैं? → रोमानिया

4 प्रश्न 4 — **सही उत्तर: A**

शिक्षण नोट

कौन-सा इंफ्रास्ट्रक्चर प्रकार पावर बंद होने पर डिस्क पर शून्य लॉग रखता है? → केवल RAM वाले सर्वर

5 प्रश्न 5 — **सही उत्तर: A**

शिक्षण नोट

VPN के बीच में कटने पर कौन-सी सुविधा कनेक्शन ब्लॉक करती है? → Kill Switch

उत्तर कुंजी: चेकपॉइंट 2 – सही या गलत

6 **प्रश्न 6** सही उत्तर: सही

शिक्षण नोट

CyberGhost का मुख्यालय रोमानिया में है, जो 14-Eyes समूह से बाहर है।

7 **प्रश्न 7** सही उत्तर: गलत

शिक्षण नोट

NoSpy सर्वर थर्ड-पार्टी व्यावसायिक डेटासेंटर से किराये पर लिए जाते हैं।

8 **प्रश्न 8** सही उत्तर: गलत

शिक्षण नोट

RAM-only सर्वर उपयोगकर्ता सेशन डेटा को स्थायी सॉलिड-स्टेट ड्राइव पर लिखते हैं।

9 **प्रश्न 9** सही उत्तर: सही

शिक्षण नोट

क्लाइंट ऐप में DNS लीक से अंतर्निहित सुरक्षा है।

10 **प्रश्न 10** सही उत्तर: सही

शिक्षण नोट

CyberGhost की ज़ीरो-लॉग्स नीति स्वतंत्र ऑडिट द्वारा सत्यापित की गई है।

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

D 1. WireGuard	F 2. AES-256	A 3. रोमानिया	G 4. NoSpy
B 5. केवल-RAM	H 6. KILL SWITCH	C 7. लीक	E 8. ऑडिट

चेकपॉइंट 3: उत्तर – प्रमुख शब्द

1 वायरगार्ड	2 सुरक्षा कवच	3 सुरक्षा नीति	4 सुरक्षित सर्वर
5 केवल रैम	6 किल स्विच		

चेकपॉइंट 6, वैकल्पिक: उत्तर – शब्द मिलान

1 G – किलस्विच	2 A – सुरक्षानीति	3 D – वायरगार्ड	4 F – केवलरैम
5 B – डीएनएसलीक	6 C – सुरक्षाकवच	7 H – सुरक्षितसर्वर	8 E – टनल

शिक्षकों के लिए चर्चा नोट

प्रमुख शब्द:
जाँचें कि क्या विद्यार्थी WireGuard, AES-256 और रोमानिया 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।

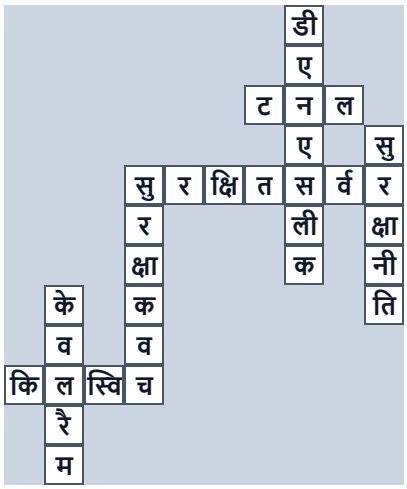
स्रोतों का मूल्यांकन:
विद्यार्थियों से वर्कशीट के स्रोतों में कम से कम एक कथन की पुष्टि करवाएँ और चर्चा करें कि आँकड़े, कीमतें और नियम समय के साथ क्यों बदल सकते हैं।

पहेलियों की कुंजियाँ और शिक्षक नोट

शब्द खोज समाधान

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

क्रॉसवर्ड समाधान



क्रॉसवर्ड समाधान के लिए शिक्षक गाइड

बाएँ से दाएँ

2 बाएँ से दाएँ: टनल आपके डिवाइस और सर्वर के बीच बना एन्क्रिप्टेड निजी रास्ता (3 अक्षर)

4 बाएँ से दाएँ: सुरक्षितसर्वर ऐसा सर्वर, जिस तक अनधिकृत पहुंच रोकने के उपाय किए गए हों (7 अक्षर)

6 बाएँ से दाएँ: किलस्विच कनेक्शन टूटने पर इंटरनेट ट्रैफ़िक काट देने वाली फेल-सेफ़ क्लाइंट यूटिलिटी (4 अक्षर)

ऊपर से नीचे

1 ऊपर से नीचे: डीएनएसलीक VPN के बाहर रिज़ॉल्वर अनुरोधों का अनचाहा उजागर होना (7 अक्षर)

3 ऊपर से नीचे: सुरक्षानीति सुरक्षा के नियमों और कदमों का लिखित ढांचा (5 अक्षर)

4 ऊपर से नीचे: सुरक्षाकवच डेटा और उपकरणों को हमलों से बचाने वाली सुरक्षा की परत (6 अक्षर)

5 ऊपर से नीचे: केवलरैम डिस्क-रहित सर्वर ढांचा, जो कोई स्थायी लॉग नहीं लिखता (5 अक्षर)

अक्षर-फेर शब्द और कूट संदेश हल कुंजी

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

शब्द अनस्क्रैम्बल कुंजी

1. नीक्षासुतिर — **सुरक्षानीति**
2. चसुक्षावकर — **सुरक्षाकवच**
3. लनट — **टनल**
4. चस्विकिल — **किलस्विच**
5. सकएनडीलीए — **डीएनएसलीक**
6. गावारर्डय — **वायरगार्ड**
7. रैमकेलव — **केवलरैम**
8. रतरसुर्वसक्षि — **सुरक्षितसर्वर**

गुप्त कूट चुनौती कुंजी

"नोस्पाई सर्वर अधिकतम डेटा गोपनीयता"

केस स्टडी के उत्तर

A केस स्टडी 1: अधिकार क्षेत्र के आधार पर गोपनीयता ऑडिट

शिक्षक समाधान

ग्रेडिंग दिशानिर्देश

छात्रों के उत्तरों में निम्नलिखित बिंदु शामिल होने चाहिए:

- परिदृश्य विश्लेषण: एक मीडिया कंपनी सुनिश्चित करना चाहती है कि उसके कॉर्पोरेट इंटेलिजेंस रिकॉर्ड विदेशी कानून प्रवर्तन द्वारा सबपीना न किए जा सकें।
- अनुशंसित रणनीति और समाधान: रोमानिया में मज़बूत गोपनीयता कानून हैं और वह Five-Eyes या Fourteen-Eyes खुफ़िया-साझेदारी नेटवर्क का सदस्य नहीं है।

B केस स्टडी 2: हार्डवेयर ज़ब्ती से सुरक्षा

शिक्षक समाधान

ग्रेडिंग दिशानिर्देश

छात्रों के उत्तरों में निम्नलिखित बिंदु शामिल होने चाहिए:

- परिदृश्य विश्लेषण: एक सर्वर सुविधा में अनधिकृत फ़िज़िकल घुसपैठ होती है और एक VPN सर्वर रैक ज़ब्त कर लिया जाता है।
- अनुशंसित रणनीति और समाधान: सर्वर RAM-only आर्किटेक्चर पर चलता है, यानी बिजली कटते ही सारा डेटा तुरंत खो जाता है।