नाम: _____ दिनांक: _____ अंक: _____

Surfshark सुरक्षा

Surfshark की सुरक्षा सुविधाओं की जाँच, जिनमें CleanWeb विज्ञापन ब्लॉकिंग, MultiHop डायनामिक रूटिंग, Nexus SDN आर्किटेक्चर, केवल-RAM सर्वर बेड़ा और Camouflage मोड शामिल हैं।

SURFSHARK सुरक्षा 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 Surfshark के सुरक्षा आर्किटेक्चर से परिचित कराता है। आप केवल-RAM सर्वर हार्डवेयर, Nexus SDN डायनामिक IP रोटेशन, CleanWeb विज्ञापन ब्लॉकर और MultiHop रूटिंग के बारे में जानेंगे।

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/surfshark/suraksha/

आपका Surfshark सुरक्षा लर्निंग रोडमैप

- Surfshark 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।

SURFSHARK 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 केवल-RAM इंफ्रास्ट्रक्चर, Nexus SDN और CleanWeb पर लागू करें। अंत में अतिरिक्त गतिविधि झटपट सोचें पूरी करें।

RAM-only सर्वर बेड़ा, Nexus SDN और CleanWeb आर्किटेक्चर (परिचय)

Surfshark केवल-RAM सर्वर बेड़े, IP Rotator के साथ Nexus सॉफ़्टवेयर-डिफ़ाइंड नेटवर्किंग, CleanWeb विज्ञापन ब्लॉकिंग और Dynamic MultiHop एन्क्रिप्शन पथों से उपयोगकर्ता की गोपनीयता की रक्षा करता है।

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

चेकपॉइंट 1: बहुविकल्पीय चुनौती

1. Surfshark के एकीकृत विज्ञापन और मैलवेयर ब्लॉकर का नाम क्या है?

- A) AdGuard
- B) CleanWeb
- C) ThreatShield
- D) NetBlocker

2. Surfshark अपने सभी सर्वरों पर कौन-सा हार्डवेयर आर्किटेक्चर इस्तेमाल करता है?

- A) हार्ड डिस्क ड्राइव
- B) 100% केवल-RAM
- C) ऑप्टिकल स्टोरेज
- D) मैग्नेटिक टेप

3. कौन-सी सुविधा ट्रैफ़िक को दो अलग VPN सर्वरों से होकर भेजती है?

- A) बायपासर
- B) MultiHop (Double VPN)
- C) Nexus नेटवर्क
- D) स्टैटिक IP

4. कौन-सी ऑब्फ़स्केशन सुविधा VPN ट्रैफ़िक को सामान्य वेब डेटा जैसा दिखाती है?

- A) Kill Switch
- B) कैमोफ़्लाज मोड
- C) CleanWeb 2.0
- D) स्प्लिट टनल

5. Surfshark Bypasser टूल का कार्य क्या है?

- A) Speed Booster
- B) स्प्लिट टनलिंग
- C) पासवर्ड मैनेजर
- D) DNS रिज़ॉल्वर

चेकपॉइंट 2: सही या गलत चुनौती

6 प्रश्न 6

6. RAM-only सर्वर रीबूट होते ही सारा परिचालन डेटा तुरंत मिटा देते हैं।

○ सही ○ गलत

7 प्रश्न 7

7. Camouflage Mode ISP को यह पता लगाने से रोकता है कि आप VPN का उपयोग कर रहे हैं।

○ सही ○ गलत

8 प्रश्न 8

8. CleanWeb 2.0 कुकी सहमति पॉपअप को ब्लॉक करने के लिए ब्राउज़र एक्सटेंशन के भीतर काम करता है।

○ सही ○ गलत

9 प्रश्न 9

9. Surfshark अस्थायी कनेक्शन टाइमस्टैम्प और बैंडविड्थ उपयोग लॉग रखता है।

○ सही ○ गलत

10 प्रश्न 10

10. Nexus नेटवर्क कनेक्शन तोड़े बिना समय-समय पर उपयोगकर्ताओं के IP पते बदलता रहता 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. परेशान करने वाले वेब विज्ञापन, ट्रैकिंग स्क्रिप्ट और फ़िशिंग लिंक _____ फ़िल्टर से ब्लॉक होते हैं।
2. सर्वर _____ मेमोरी में चलते हैं, इसलिए उपयोगकर्ता गतिविधि कोई फ़ॉरेंसिक निशान नहीं छोड़ती।
3. उपयोगकर्ता और सर्वर के बीच एन्क्रिप्टेड रास्ता बनाने वाली _____ बाहरी निगरानी रोकती है।
4. इंटरनेट पर डेटा भेजते समय पूरे नेटवर्क की _____ एन्क्रिप्शन से मज़बूत बनाया जाता है।
5. बैंकिंग ऐप को VPN टनल बायपास करने देना _____ सेटिंग से प्रबंधित होता है।
6. सर्वर बेड़े को जोड़ने वाला अगली पीढ़ी का SDN आर्किटेक्चर _____ प्रणाली है।

शब्दावली शब्द-बैंक

कनेक्शन सुरक्षा | क्लीन वेब | नेक्सस | बायपासर | मल्टीहॉप | रैम ओनली | रोटेटिंग | सुरक्षित टनल

अपने उत्तर यहाँ लिखें:

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

चेकपॉइंट 4: VPN और नेटवर्क अवधारणा मिलान

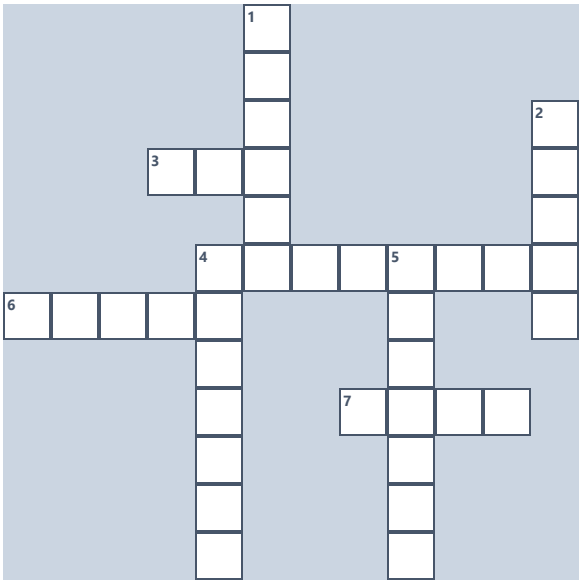
परिभाषा मिलान

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. क्लीनवेब**	**A**	स्वचालित सुरक्षा सुविधा जो VPN बंद होने पर नेटवर्क ट्रैफ़िक ब्लॉक कर देती है।
☐	**2. रैमओनली**	**B**	स्प्लिट-टनलिंग की वह कार्यक्षमता जो चुने हुए एप्लिकेशन को VPN बायपास करने देती है।
☐	**3. मल्टीहॉप**	**C**	उन्नत फ़िल्टर जो विज्ञापन, मैलवेयर और कुकी सहमति बैनर को ब्लॉक करता है।
☐	**4. कनेक्शनसुरक्षा**	**D**	वोलेटाइल मेमोरी सर्वर हार्डवेयर जो हर पावर साइकल पर सारा डेटा मिटा देता है।
☐	**5. बायपासर**	**E**	ऐसी सुविधा जो टनल को बाधित किए बिना आपका बाहरी IP पता नियमित रूप से बदलती है।
☐	**6. नेक्सस**	**F**	VPN सिग्नेचर छिपाकर सामान्य HTTPS ट्रैफ़िक की नकल करने वाली ऑब्फ़स्केशन तकनीक।
☐	**7. Nexus नेट**	**G**	डबल-VPN रूटिंग सुविधा जो ट्रैफ़िक को दो अलग सर्वर नोड से होकर एन्क्रिप्ट करती है।
☐	**8. रोटेटिंग**	**H**	स्वामित्व वाला सॉफ़्टवेयर-परिभाषित नेटवर्क जो सभी सर्वरों को एक एकीकृत मेश में जोड़ता 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

3. अपना सॉफ़्टवेयर-परिभाषित नेटवर्क, जो सभी सर्वरों को एकीकृत मेश में जोड़ता है (3)

4. एन्क्रिप्टेड माध्यम से बना भरोसेमंद इंटरनेट जुड़ाव। (8)

6. स्प्लिट-टनलिंग सुविधा, जो चुनिंदा ऐप को VPN बायपास करने देती है (5)

7. उन्नत फ़िल्टर, जो विज्ञापन, मैलवेयर और कुकी सहमति बैनर ब्लॉक करता है (4)

ऊपर से नीचे

1. ऐसा सर्वर जो डेटा केवल अस्थायी मेमोरी में रखता है। (6)

2. वोलाटाइल मेमोरी वाला सर्वर हार्डवेयर, जो हर पावर साइकिल पर सारा डेटा मिटा देता है (5)

4. उपयोगकर्ता और सर्वर के बीच एन्क्रिप्टेड रास्ता। (7)

5. इंटरनेट से जुड़ने की पूरी प्रक्रिया को हमलों से बचाना। (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: अपना सॉफ़्टवेयर-परिभाषित नेटवर्क, जो सभी सर्वरों को एकीकृत मेश में जोड़ता है (3 अक्षर):

4 बाएँ से दाएँ: एन्क्रिप्टेड माध्यम से बना भरोसेमंद इंटरनेट जुड़ाव। (8 अक्षर):

6 बाएँ से दाएँ: स्प्लिट-टनलिंग सुविधा, जो चुनिंदा ऐप को VPN बायपास करने देती है (5 अक्षर):

7 बाएँ से दाएँ: उन्नत फ़िल्टर, जो विज्ञापन, मैलवेयर और कुकी सहमति बैनर ब्लॉक करता है (4 अक्षर):

ऊपर से नीचे

1 ऊपर से नीचे: ऐसा सर्वर जो डेटा केवल अस्थायी मेमोरी में रखता है। (6 अक्षर):

2 ऊपर से नीचे: वोलाटाइल मेमोरी वाला सर्वर हार्डवेयर, जो हर पावर साइकिल पर सारा डेटा मिटा देता है (5 अक्षर):

4 ऊपर से नीचे: उपयोगकर्ता और सर्वर के बीच एन्क्रिप्टेड रास्ता। (7 अक्षर):

5 ऊपर से नीचे: इंटरनेट से जुड़ने की पूरी प्रक्रिया को हमलों से बचाना। (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	रै	रे	स	ख	नि	फ	ढ	मा
ना	का	रे	दे	सि	मी	क	म	मे	पि	ता	ति	ज	श	भ
ऊ	अ	ऊ	ए	रि	वि	श	ओ	य	मो	वि	व	वा	पा	ल
च	से	स	कि	य	ब	वे	न	क्ली	घ	री	प	के	की	व
सि	री	क्स	त	की	सु	कि	ली	सि	ना	बा	स	ने	पा	ते
क्षा	ण	ने	ए	ता	र	सा	सु	मी	न	नी	य	र्व	ऋ	ले
र	घ	ति	जि	ला	क्षि	ए	जी	र	ले	ड	ल	पा	र	द
सु	जे	घ	के	च	त	से	दे	री	क्षि	ए	पी	उ	स	अ
न	जे	मि	घ	व	क	आ	च	मी	च	त	ट	थ	फ	र
क्श	ग	ना	सी	का	ने	ज	फ	नी	जी	ता	ट	ठ	से	लि
ने	ट	आ	इ	से	क्श	रा	के	री	पा	वा	सि	न	य	नि
क	पि	ने	ख	के	न	वे	ऊ	ड	नी	दे	दि	भ	ल	आ
नि	जे	वे	वे	ष	ण	प	कि	से	य	ह	ह	ते	रा	द
सा	सी	थ	जे	इ	मे	ला	ढ	पे	ऋ	वे	नी	वे	उ	थ
ह	जे	त	य	मी	रे	मि	दि	ए	ह	जे	जा	ढ	वी	रा

शब्दावली शब्द-सूची

क्लीनवेब, रैमओनली, सुरक्षितटनल, कनेक्शनसुरक्षा, बायपासर, नेक्सस, सुरक्षितकनेक्शन, मेमोरीसर्वर

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	परिभाषाएँ और मिलान फ़ील्ड
A. क्लीनवेब	1. इंटरनेट से जुड़ने की पूरी प्रक्रिया को हमलों से बचाना।
B. रैमओनली	2. अपना सॉफ़्टवेयर-परिभाषित नेटवर्क, जो सभी सर्वरों को एकीकृत मेश में जोड़ता है।
C. सुरक्षितटनल	3. उन्नत फ़िल्टर, जो विज्ञापन, मैलवेयर और कुकी सहमति बैनर ब्लॉक करता है।
D. कनेक्शनसुरक्षा	4. स्प्लिट-टनलिंग सुविधा, जो चुनिंदा ऐप को VPN बायपास करने देती है।
E. बायपासर	5. वोलाटाइल मेमोरी वाला सर्वर हार्डवेयर, जो हर पावर साइकिल पर सारा डेटा मिटा देता है।
F. नेक्सस	6. ऐसा सर्वर जो डेटा केवल अस्थायी मेमोरी में रखता है।
G. सुरक्षितकनेक्शन	7. उपयोगकर्ता और सर्वर के बीच एन्क्रिप्टेड रास्ता।
H. मेमोरीसर्वर	8. एन्क्रिप्टेड माध्यम से बना भरोसेमंद इंटरनेट जुड़ाव।

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. **वे क्ली ब न** _____

2. **सु क्षि ल न ट त र** _____

3. **पा बा र स य** _____

4. **त क्श न ने क सु र क्षि** _____

5. **ओ ली रै न म** _____

6. **र क्श सु क न क्षा ने** _____

7. **स क्स ने** _____

8. **री र मे र्व स मो** _____

अतिरिक्त गतिविधि: झटपट सोचें

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

1	Surfshark की सुरक्षा सुविधाएँ			
2	आपका VPN कनेक्शन धीमा होने के संकेत			
3	आपके जाने-पहचाने VPN प्रोटोकॉल			
4	ऐसी चीज़ें जिन्हें एन्क्रिप्शन सुरक्षित रखता है			
5	सार्वजनिक Wi-Fi पर खतरे			
6	मज़बूत गोपनीयता कानूनों के लिए जाने जाने वाले देश			
7	मज़बूत पासवर्ड बनाने के तरीके			
8	ऐसे डिवाइस जिन पर आप Surfshark इंस्टॉल करेंगे			
9	Surfshark कस्टमर सपोर्ट के लिए सवाल			
10	अतिरिक्त सुरक्षा के लिए आप जो सेटिंग्स चालू करते हैं			
11	ऐसी चीज़ें जिन्हें Surfshark आपके नेटवर्क से छिपा सकता है			
12	VPN लीक के प्रकार			
13	ऐसा डेटा जिसे VPN को कभी स्टोर नहीं करना चाहिए			
14	एक अच्छे VPN ऐप का वर्णन करने वाले शब्द			
15	ऐसी चीज़ें जिन्हें ऑडिट जाँच सकता है			

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: कैंपस और कार्यस्थल फ़िल्टर को बायपास करना



परिदृश्य: एक छात्र पाता है कि उसके विश्वविद्यालय कैंपस का Wi-Fi सभी मानक OpenVPN और WireGuard पोर्ट ब्लॉक करता है।

चर्चा प्रश्न: Surfshark की कौन-सी सुविधा छात्र को नेटवर्क एडमिनिस्ट्रेटरों की नज़र में आए बिना कनेक्ट होने देती है?

केस स्टडी 2: उच्च जोखिम वाली खोजी पत्रकारिता



परिदृश्य: एक खोजी पत्रकार को संवेदनशील कॉर्पोरेट रिकॉर्ड पर शोध करते समय निगरानी के विरुद्ध अतिरिक्त सुरक्षा चाहिए।

चर्चा प्रश्न: Dynamic MultiHop एकल-सर्वर रूटिंग की तुलना में बेहतर गोपनीयता कैसे देता 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	52	13	61	44	44		39	54	23	52	23	47	57	15		2	4	33	48

15	54	33	32	48	38	28	46		35	26	60	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: Surfshark CleanWeb क्या है?

CleanWeb एक एकीकृत सुरक्षा सुविधा है जो विज्ञापनों, ट्रैकरों, मैलवेयर और फ़िशिंग साइटों को ब्लॉक करती है।

Q2: RAM-only सर्वर क्या हैं?

RAM-only सर्वर वोलाटाइल मेमोरी पर चलते हैं, यानी मेमोरी में रखा डेटा सर्वर रीबूट होने पर मिट जाता है।

Q3: Surfshark MultiHop क्या है?

MultiHop (Double VPN) आपके इंटरनेट कनेक्शन को दो अलग सर्वर स्थानों से रूट और एन्क्रिप्ट करता है।

Q4: Camouflage Mode कैसे काम करता है?

Camouflage Mode VPN ट्रैफ़िक को ऑब्फ़स्केट करता है ताकि आपका ISP यह न जान सके कि आप VPN का उपयोग कर रहे हैं।

Q5: Bypasser फ़ीचर क्या है?

Bypasser, Surfshark का स्प्लिट टनलिंग टूल है जो चुनिंदा ऐप्स या वेबसाइटों को VPN को बायपास करने देता है।

चेकपॉइंट 10: बुनियादी VPN FAQ (भाग B)

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

Q6: क्या Surfshark में Kill Switch है?

हाँ, VPN अचानक गिरने पर Kill Switch आपको इंटरनेट से डिस्कनेक्ट कर देता है।

Q7: Surfshark कौन-सा एन्क्रिप्शन मानक उपयोग करता है?

Surfshark AES-256-GCM और ChaCha20 का उपयोग करता है, साथ ही अपने नए Dausos प्रोटोकॉल पर AEGIS-256X2 का।

Q8: क्या Surfshark की नो-लॉग्स नीति का ऑडिट हुआ है?

हाँ, Deloitte ने 2023 में और फिर 2025 में Surfshark की नो-लॉग नीति सत्यापित की।

Q9: Surfshark Nexus क्या है?

Nexus उन्नत SDN आर्किटेक्चर है, जो ज़्यादा सुचारू रूटिंग के लिए सभी सर्वरों को एक एकीकृत नेटवर्क में जोड़ता है।

Q10: IP Rotator फ़ीचर क्या है?

IP Rotator, आपका VPN सत्र डिस्कनेक्ट किए बिना हर कुछ मिनट में आपका IP पता अपने-आप बदलता है।

चेकपॉइंट 10: उन्नत VPN FAQ (भाग C)

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

Q1: Dynamic MultiHop पारंपरिक Double VPN से कैसे अलग है?

Dynamic MultiHop आपको दुनिया भर के एंट्री और एग्ज़िट सर्वरों का कोई भी संयोजन कस्टमाइज़ करने देता है।

Q2: क्या CleanWeb 2.0 ब्राउज़र एक्सटेंशन पर काम करता है?

हाँ, CleanWeb 2.0 Chrome/Firefox के भीतर वीडियो विज्ञापन, कुकी सहमति पॉपअप और अलर्ट बैनर ब्लॉक करता है।

Q3: सिक्योरिटी सुइट में Alternative ID क्या है?

Alternative ID अनूठे व्यक्तिगत छद्म नाम, ईमेल पते और फ़ोन मास्क बनाता है।

Q4: Surfshark DNS लीक कैसे रोकता है?

Surfshark सभी डोमेन अनुरोधों को हर नोड पर अपने निजी DNS सर्वरों से रूट करता है।

Q5: क्या Surfshark मोबाइल पर ChaCha20 एन्क्रिप्शन सपोर्ट करता है?

हाँ, बेहतर मोबाइल दक्षता के लिए Android और iOS पर WireGuard, ChaCha20-Poly1305 का उपयोग करता है।

चेकपॉइंट 10: उन्नत VPN FAQ (भाग D)

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

Q6: Surfshark में NoBorders मोड क्या है?

NoBorders प्रतिबंधात्मक नेटवर्क माहौल का अपने आप पता लगा लेता है और विशेष सर्वर उपलब्ध कराता है।

Q7: Surfshark ब्राउज़र एक्सटेंशन का सुरक्षा ऑडिट किसने किया?

स्वतंत्र साइबर सुरक्षा फ़र्म Cure53 ने ब्राउज़र एक्सटेंशन और सर्वर सिस्टम के ऑडिट पूरे किए।

Q8: Surfshark IPv6 लीक से कैसे बचाता है?

Surfshark IPv6 ट्रैफ़िक को सुरक्षित रूप से रूट करता है या किसी भी अनएन्क्रिप्टेड लीक को रोकने के लिए उसे सुरक्षित रूप से प्रतिबंधित करता है।

Q9: Surfshark का क़ानूनी अधिकार क्षेत्र कहाँ स्थित है?

Surfshark नीदरलैंड्स के कानून के अंतर्गत काम करता है और सख़्त GDPR यूरोपीय गोपनीयता मानकों का पालन करता है।

Q10: क्या Surfshark टू-फ़ैक्टर ऑथेंटिकेशन (2FA) को सपोर्ट करता है?

हाँ, और Surfshark One एक 2FA लॉक जोड़ता है ताकि केवल आप ही सुविधा सेटिंग्स बदल सकें।

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

1. Surfshark के अनुसार उसका पूरा 4,500+ सर्वर नेटवर्क बिना डिस्क वाले, वोलेटाइल केवल-RAM हार्डवेयर पर चलता है।

2. VPN इनसाइट

2. बिग फ़ोर फ़र्म Deloitte ने 2023 में और फिर नवंबर 2025 में Surfshark की नो-लॉग्स नीति सत्यापित की।

3. VPN इनसाइट

3. स्वामित्व वाला Nexus आर्किटेक्चर सभी वैश्विक सर्वरों को एक गतिशील सॉफ़्टवेयर-परिभाषित नेटवर्क में जोड़ता है।

4. VPN इनसाइट

4. Rotating IP, VPN कनेक्शन टूटे बिना लगभग हर पाँच मिनट में आपका IP पता बदल देता है।

5. VPN इनसाइट

5. CleanWeb 2.0 ब्राउज़र में घुसपैठिए कुकी सहमति पॉपअप और वीडियो विज्ञापनों को सीधे ब्लॉक करता है।

6. VPN इनसाइट

6. Dynamic MultiHop उपयोगकर्ताओं को 100 देशों में अनुकूलित डुअल-सर्वर एन्क्रिप्शन पाथ बनाने देता है।

7. VPN इनसाइट

7. Camouflage Mode VPN हेडर सिग्नेचर हटा देता है, जिससे ट्रैफ़िक सामान्य HTTPS से अलग नहीं दिखता।

8. VPN इनसाइट

8. Alternative ID डेटाबेस लीक से उपयोगकर्ताओं को बचाने के लिए अस्थायी छद्म नाम और ईमेल मास्क बनाता है।

9. VPN इनसाइट

9. Surfshark WireGuard प्रोटोकॉल पर ChaCha20 के साथ AES-256-GCM सममित एन्क्रिप्शन लागू करता है।

10. VPN इनसाइट

10. NoBorders मोड प्रतिबंधित नेटवर्क पर अपने-आप सक्रिय होकर लचीली टनलिंग पहुँच देता है।

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] Surfshark. (n.d.). Welcome to Surfshark's trust center!
https://surfshark.com/trust-center

[2] Surfshark. (2025). Our no-logs policy was verified again.
https://surfshark.com/blog/deloitte-nologs-policy-verified-again

[3] Surfshark. (n.d.). Surfshark VPN protocols: Dausos, WireGuard, OpenVPN, IKEv2.
https://surfshark.com/features/surfshark-vpn-protocols

[4] Surfshark. (n.d.). Clean Web: VPN ad blocker for safe and ad-free browsing.
https://surfshark.com/features/cleanweb

[5] Surfshark. (n.d.). What is double VPN and when to use it.
https://surfshark.com/features/multihop

[6] Surfshark. (n.d.). Rotating IP: rotate your IP for extra privacy.
https://surfshark.com/features/ip-rotator

[7] Surfshark. (n.d.). Surfshark Privacy Policy.
https://surfshark.com/privacy

[8] Surfshark. (n.d.). Surfshark VPN servers: location list.
https://surfshark.com/servers

[9] Surfshark. (n.d.). VPN kill switch: protection that never slips.
https://surfshark.com/features/kill-switch

[10] Surfshark. (2023). Surfshark server infrastructure undergoes an independent audit.
https://surfshark.com/blog/surfshark-server-infrastructure-undergoes-independent-audit

[11] Surfshark. (n.d.). Alternative ID & Alternative Number.
https://surfshark.com/alternative-id

[12] Surfshark. (n.d.). What are obfuscated servers & why you need them.
https://surfshark.com/features/obfuscated-servers

उत्तर कुंजी: चेकपॉइंट 1 – बहुविकल्पीय

1 **इंटीग्रेटेड कंटेंट ब्लॉकर** विज्ञापन और मैलवेयर सुरक्षा — **सही उत्तर: B**

शिक्षण नोट

CleanWeb Surfshark का एकीकृत सुरक्षा फ़िल्टर है, जो नेटवर्क स्तर पर विज्ञापनों, ट्रैकर डोमेन, फ़िशिंग वेबसाइटों और हानिकारक URL स्क्रिप्ट को ब्लॉक करता है। उद्धरण: CleanWeb Security Specs।

2 **100% केवल-RAM इंफ्रास्ट्रक्चर** RAM आर्किटेक्चर — **सही उत्तर: B**

शिक्षण नोट

Surfshark केवल-RAM सर्वर चलाता है, इसलिए सर्वर मेमोरी में रखा डेटा सर्वर बंद या रीबूट होने पर मिट जाता है। उद्धरण: Cure53 Infrastructure Audit।

3 **MultiHop डबल टनलिंग** मल्टीहॉप VPN — **सही उत्तर: B**

शिक्षण नोट

MultiHop (Double VPN) ट्रैफ़िक सहसंबंध हमलों को रोकने के लिए अलग-अलग देशों के दो अलग सर्वर नोड से ट्रैफ़िक को एन्क्रिप्ट करता है। संदर्भ: Surfshark MultiHop Guide।

4 **Camouflage Mode ऑब्फ़स्केशन** ऑब्फ़स्केशन — **सही उत्तर: B**

शिक्षण नोट

Camouflage Mode OpenVPN पैकेट हेडर बदलकर VPN ट्रैफ़िक को सामान्य HTTPS ट्रैफ़िक जैसा दिखाता है, जिससे प्रतिबंधात्मक फ़ायरवॉल ब्लॉक को बायपास किया जा सकता है। उद्धरण: Surfshark Stealth Whitepaper।

5 **Bypasser स्प्लिट टनलिंग** स्प्लिट टनलिंग — **सही उत्तर: B**

शिक्षण नोट

Bypasser, Surfshark का स्प्लिट टनलिंग टूल है जो उपयोगकर्ताओं को चुनिंदा ऐप्स या वेबसाइटें चुनने देता है, जिन्हें सीधे उनके सामान्य ISP कनेक्शन से रूट किया जाता है। उद्धरण: Surfshark Client Features।

उत्तर कुंजी: चेकपॉइंट 2 – सही या गलत

6 **वोलेटाइल मेमोरी डेटा वाइप** सर्वर सुरक्षा — **सही उत्तर: सही**

शिक्षण नोट

RAM-only सर्वर स्थायी हार्ड ड्राइव पर कोई डेटा नहीं रखते; हार्डवेयर रीबूट करने पर सारी परिचालन मेमोरी तुरंत साफ़ हो जाती है। स्रोत: RAM Server Architecture।

7 **Camouflage Mode द्वारा ISP से छिपाव** ट्रैफ़िक छिपाव — **सही उत्तर: सही**

शिक्षण नोट

Camouflage Mode OpenVPN प्रोटोकॉल सिग्नेचर हटा देता है, जिससे ISP यह पता नहीं लगा पाते कि उपयोगकर्ता VPN टनल से जुड़ा है। उद्धरण: Deep Packet Inspection Guide।

8 **CleanWeb 2.0 ब्राउज़र एक्सटेंशन** ब्राउज़र एक्सटेंशन — **सही उत्तर: सही**

शिक्षण नोट

CleanWeb 2.0 ब्राउज़र एक्सटेंशन के भीतर काम करता है और रीयल-टाइम में कुकी सहमति पॉपअप, वीडियो विज्ञापन और हानिकारक रीडायरेक्ट स्क्रिप्ट को ब्लॉक करता है। उद्धरण: CleanWeb 2.0 Release Notes।

9 **शून्य कनेक्शन लॉग रिटेंशन** नो-लॉग्स नीति — **सही उत्तर: गलत**

शिक्षण नोट

Surfshark स्वतंत्र रूप से ऑडिट की गई सख़्त ज़ीरो-लॉग नीति रखता है और कोई IP पता, कनेक्शन टाइमस्टैम्प या बैंडविड्थ लॉग रिकॉर्ड नहीं करता। उद्धरण: Deloitte No-Logs Audit।

10 **Nexus IP डायनामिक रोटेशन** Nexus नेटवर्क — **सही उत्तर: सही**

शिक्षण नोट

Surfshark Nexus सॉफ़्टवेयर-डिफ़ाइंड नेटवर्क सक्रिय VPN कनेक्शन तोड़े बिना हर कुछ मिनट में उपयोगकर्ताओं के IP पते गतिशील रूप से बदलता है। उद्धरण: Surfshark Nexus Architecture।

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

C 1. क्लीनवेब	D 2. रैमओनली	G 3. मल्टीहॉप	F 4. कनेक्शनसुरक्षा
B 5. बायपासर	A 6. नेक्सस	H 7. Nexus नेट	E 8. रोटेटिंग

चेकपॉइंट 3: उत्तर – प्रमुख शब्द

1 क्लीन वेब	2 रैम ओनली	3 सुरक्षित टनल	4 कनेक्शन सुरक्षा
5 बायपासर	6 नेक्सस		

चेकपॉइंट 6, वैकल्पिक: उत्तर – शब्द मिलान

1 D – कनेक्शनसुरक्षा	2 F – नेक्सस	3 A – क्लीनवेब	4 E – बायपासर
5 B – रैमओनली	6 H – मेमोरीसर्वर	7 C – सुरक्षितटनल	8 G – सुरक्षितकनेक्शन

शिक्षकों के लिए चर्चा नोट

प्रमुख शब्द:
जाँचें कि क्या विद्यार्थी क्लीनवेब, रैमओनली और मल्टीहॉप 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।

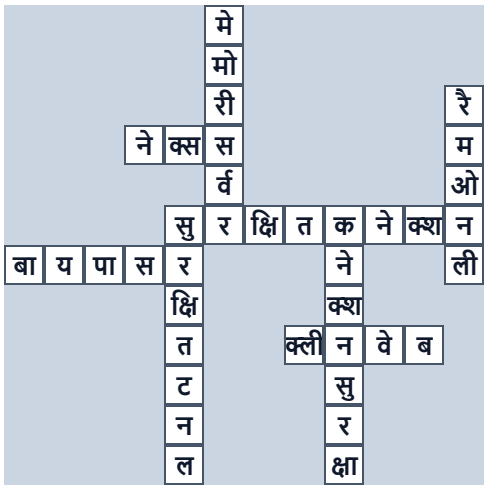
स्रोतों का मूल्यांकन:
विद्यार्थियों से वर्कशीट के स्रोतों में कम से कम एक कथन की पुष्टि करवाएँ और चर्चा करें कि आँकड़े, कीमतें और नियम समय के साथ क्यों बदल सकते हैं।

पहेलियों की कुंजियाँ और शिक्षक नोट

शब्द खोज समाधान

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

क्रॉसवर्ड समाधान



क्रॉसवर्ड समाधान के लिए शिक्षक गाइड

बाएँ से दाएँ

3 बाएँ से दाएँ: नेक्सस अपना सॉफ़्टवेयर-परिभाषित नेटवर्क, जो सभी सर्वरों को एकीकृत मेश में जोड़ता है (3 अक्षर)

4 बाएँ से दाएँ: सुरक्षितकनेक्शन एन्क्रिप्टेड माध्यम से बना भरोसेमंद इंटरनेट जुड़ाव। (8 अक्षर)

6 बाएँ से दाएँ: बायपासर स्प्लिट-टनलिंग सुविधा, जो चुनिंदा ऐप को VPN बायपास करने देती है (5 अक्षर)

7 बाएँ से दाएँ: क्लीनवेब उन्नत फ़िल्टर, जो विज्ञापन, मैलवेयर और कुकी सहमति बैनर ब्लॉक करता है (4 अक्षर)

ऊपर से नीचे

1 ऊपर से नीचे: मेमोरीसर्वर ऐसा सर्वर जो डेटा केवल अस्थायी मेमोरी में रखता है। (6 अक्षर)

2 ऊपर से नीचे: रैमओनली वोलाटाइल मेमोरी वाला सर्वर हार्डवेयर, जो हर पावर साइकिल पर सारा डेटा मिटा देता है (5 अक्षर)

4 ऊपर से नीचे: सुरक्षितटनल उपयोगकर्ता और सर्वर के बीच एन्क्रिप्टेड रास्ता। (7 अक्षर)

5 ऊपर से नीचे: कनेक्शनसुरक्षा इंटरनेट से जुड़ने की पूरी प्रक्रिया को हमलों से बचाना। (7 अक्षर)

अक्षर-फेर शब्द और कूट संदेश हल कुंजी

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

शब्द अनस्क्रैम्बल कुंजी

1. वेक्लीबन — **क्लीनवेब**
2. सुक्षिलनटतर — **सुरक्षितटनल**
3. पाबारसय — **बायपासर**
4. तक्शननेकसुरक्षि — **सुरक्षितकनेक्शन**
5. ओलीरैनम — **रैमओनली**
6. रक्शसुकनक्षाने — **कनेक्शनसुरक्षा**
7. सक्सने — **नेक्सस**
8. रीरमेर्वसमो — **मेमोरीसर्वर**

गुप्त कूट चुनौती कुंजी

"नेक्सस रोटेटिंग आईपी गोपनीयता बढ़ाता"

केस स्टडी के उत्तर

A केस स्टडी 1: कैंपस और कार्यस्थल फ़िल्टर को बायपास करना

शिक्षक समाधान

ग्रेडिंग रूब्रिक और समाधान दिशानिर्देश

- परिदृश्य विश्लेषण: एक छात्र पाता है कि उसकी यूनिवर्सिटी कैंपस का Wi-Fi सभी मानक OpenVPN और WireGuard पोर्ट ब्लॉक करता है।
- फ़ोकस प्रश्न: Surfshark की कौन-सी सुविधा छात्र को नेटवर्क व्यवस्थापकों की नज़र में आए बिना कनेक्ट करने देती है?
- अनुशंसित रणनीति और समाधान: Camouflage Mode (OpenVPN) चालू करें, जो VPN मेटाडेटा को छिपाता है ताकि फ़ायरवॉल को सामान्य HTTPS ब्राउज़िंग दिखे।

B केस स्टडी 2: उच्च जोखिम वाली खोजी पत्रकारिता

शिक्षक समाधान

ग्रेडिंग रूब्रिक और समाधान दिशानिर्देश

- परिदृश्य विश्लेषण: एक खोजी पत्रकार को संवेदनशील कॉर्पोरेट रिकॉर्ड पर शोध करते समय निगरानी से अतिरिक्त सुरक्षा चाहिए।
- फ़ोकस प्रश्न: सिंगल-सर्वर राउटिंग की तुलना में Dynamic MultiHop बेहतर गोपनीयता कैसे देता है?
- अनुशंसित रणनीति और समाधान: Dynamic MultiHop ट्रैफ़िक को दो देशों के एंट्री और एग्ज़िट सर्वरों से गुज़ारता है, इसलिए कोई एक सर्वर उपयोगकर्ता को उजागर नहीं कर सकता।