नाम: _____ दिनांक: _____ अंक: _____

Avast SecureLine VPN

Avast SecureLine VPN की लॉगिंग नीतियों, प्रोप्राइटरी प्रोटोकॉल और प्लेटफ़ॉर्म प्रदर्शन का मूल्यांकन।

Avast SecureLine VPN समीक्षा 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 Avast SecureLine VPN की तकनीकी समीक्षा से परिचित कराता है। आप चेक क्षेत्राधिकार, Mimic मालिकाना प्रोटोकॉल, AES-256 मानक एन्क्रिप्शन, लॉगिंग नीतियाँ और क्लाइंट फ़ीचर 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/avast-secureline-vpn/

आपका Avast SecureLine VPN लर्निंग रोडमैप

- Avast की लॉगिंग नीति और टेलीमेट्री डेटा एकत्रीकरण का विश्लेषण करें।
- Mimic और OpenVPN प्रोटोकॉल के प्रदर्शन का मूल्यांकन करें।
- वैश्विक सर्वर नेटवर्क के आकार और IP पते की विविधता का नक्शा बनाएँ।
- कनेक्शन लेटेंसी और गति हानि के अनुपात की तुलना करें।
- Windows और macOS पर SecureLine क्लाइंट इंस्टॉल और कॉन्फ़िगर करें।
- DNS लीक सुरक्षा और स्मार्ट रूटिंग नियमों का ऑडिट करें।

Avast SecureLine VPN 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 चेक कानूनी क्षेत्राधिकार और Mimic प्रोटोकॉल पर लागू करें। अंत में अतिरिक्त गतिविधि झटपट सोचें पूरी करें।

चेक कानूनी अधिकार क्षेत्र और Mimic प्रोटोकॉल (परिचय)

Avast SecureLine VPN उपयोगकर्ता कनेक्शन की सुरक्षा के लिए अपने मालिकाना Mimic प्रोटोकॉल और मानक AES-256 एन्क्रिप्शन का उपयोग करता है। चेक क्षेत्राधिकार में काम करते हुए यह EU के डेटा नियमों का पालन करता है और अनुकूलित स्ट्रीमिंग तथा शेयरिंग सर्वर देता है।

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

चेकपॉइंट 1: बहुविकल्पीय चुनौती

1. Avast SecureLine के स्वामित्व वाले कनेक्शन प्रोटोकॉल का नाम क्या है?

- A) Mimic
- B) NordLynx
- C) Lightway
- D) Stealth

2. Avast का आधिकारिक मुख्यालय कहाँ है?

- A) चेक गणराज्य
- B) संयुक्त राज्य अमेरिका
- C) स्विट्ज़रलैंड
- D) पनामा

3. Avast SecureLine VPN डिफ़ॉल्ट रूप से कौन-सा एन्क्रिप्शन मानक इस्तेमाल करता है?

- A) AES-256
- B) ChaCha20
- C) Blowfish
- D) DES

4. मल्टी-डिवाइस प्लान कितने एक साथ डिवाइस लिंक की अनुमति देता है?

- A) दस लिंक
- B) पाँच लिंक
- C) दो लिंक
- D) असीमित लिंक

5. Avast अपनी नीति में कौन-सा सत्र मीट्रिक लॉग करना स्वीकार करता है?

- A) कनेक्शन टाइमस्टैम्प
- B) देखे गए URL
- C) प्रेषित फ़ाइलें
- D) खोज क्वेरी

चेकपॉइंट 2: सही या गलत चुनौती

6 प्रश्न 6

6. Avast SecureLine VPN सेंसरशिप ब्लॉकिंग को बायपास करने के लिए Mimic प्रोटोकॉल का उपयोग करता है।

○ सही ○ गलत

7 प्रश्न 7

7. Avast VPN का सर्वर आर्किटेक्चर पूरी तरह ऑडिट किया हुआ, ज़ीरो-लॉग्स वाला है।

○ सही ○ गलत

8 प्रश्न 8

8. SecureLine VPN P2P फ़ाइल शेयरिंग के लिए अनुकूलित समर्पित सर्वर देता है।

○ सही ○ गलत

9 प्रश्न 9

9. चेक गणराज्य का क्षेत्राधिकार EU के डेटा रिटेंशन कानूनों से पूरी तरह मुक्त है।

○ सही ○ गलत

10 प्रश्न 10

10. Avast VPN में Windows और macOS दोनों पर सिस्टम-व्यापी Kill Switch शामिल 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. Avast SecureLine का मुख्य उद्देश्य सार्वजनिक वाई-फ़ाई पर उपयोगकर्ता की ऑनलाइन _____ बढ़ाना है।

2. Avast SecureLine उपयोगकर्ताओं को अलग-अलग देशों में अपना _____ चुनने की सुविधा देता है।

3. ट्रैफ़िक का पेलोड डेटा मानक _____ एल्गोरिद्म से सुरक्षित किया जाता है।

4. बहु-डिवाइस सदस्यता योजना में एक साथ अधिकतम _____ जुड़ सकते हैं।

5. Avast की गोपनीयता नीति के अनुसार वह क्षमता प्रबंधन के लिए हर _____ का समय दर्ज करता है।

6. बहु-उपकरण सदस्यता में एक साथ जुड़ने वाले उपकरणों की _____ योजना के अनुसार तय होती है।

शब्दावली शब्द-बैंक

एईएस एन्क्रिप्शन | ओवरहेड | कनेक्शन सर्वर स्थान | टाइमस्टैम्प सुरक्षा | डिवाइस सीमा | दस डिवाइस

अपने उत्तर यहाँ लिखें:

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

चेकपॉइंट 4: प्रमुख अवधारणा मिलान

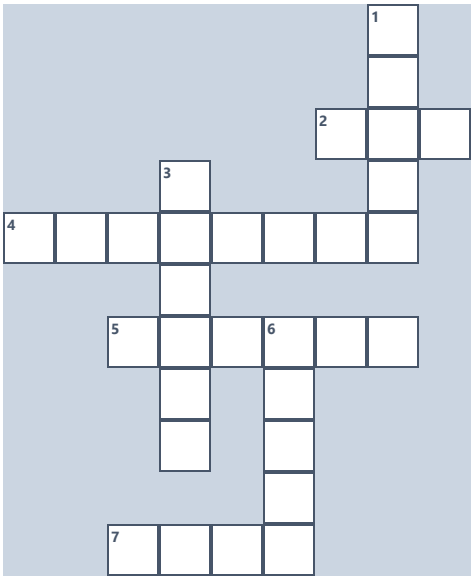
परिभाषा मिलान

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. Mimic**	**A**	एन्क्रिप्शन की CPU प्रोसेसिंग लागत।
☐	**2. चेक गणराज्य**	**B**	औद्योगिक-स्तर का एन्क्रिप्शन मानक।
☐	**3. AES-256**	**C**	लीक रोकने वाला स्थानीय फ़ायरवॉल नियम।
☐	**4. दस डिवाइस**	**D**	स्वामित्व वाला Avast VPN प्रोटोकॉल।
☐	**5. टाइमस्टैम्प**	**E**	मल्टी-डिवाइस सदस्यता का लिंक सीमा।
☐	**6. KILL SWITCH**	**F**	मध्य यूरोपीय कानूनी अधिकार क्षेत्र।
☐	**7. पीयर-टू-पीयर**	**G**	लॉग किए गए सेशन कनेक्शन मीट्रिक।
☐	**8. ओवरहेड**	**H**	साझा करने के लिए समर्पित सर्वर श्रेणियाँ।

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. ऑनलाइन डेटा और पहचान को खतरों तथा अनधिकृत पहुंच से बचाए रखने की स्थिति (3)

4. औद्योगिक स्तर का एन्क्रिप्शन मानक (8)

5. सक्रिय डिवाइस सत्रों की संख्या को सीमित करने वाली बाध्यता (6)

7. डिवाइस और सर्वर या नेटवर्क के बीच बना संपर्क, जिससे डेटा का आदान-प्रदान होता है (4)

ऊपर से नीचे

1. वह देश या शहर, जहां वीपीएन सर्वर भौतिक रूप से स्थित है और जिससे आपका आईपी दिखता है (5)

3. एक साथ कई डिवाइस जोड़ने वाली सदस्यता की सीमा (6)

6. नियमित शुल्क पर मिलने वाली सेवा की सदस्यता, जैसे मासिक या वार्षिक योजना (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: ऑनलाइन डेटा और पहचान को खतरों तथा अनधिकृत पहुंच से बचाए रखने की स्थिति (3 अक्षर):

4 बाएँ से दाएँ: औद्योगिक स्तर का एन्क्रिप्शन मानक (8 अक्षर):

5 बाएँ से दाएँ: सक्रिय डिवाइस सत्रों की संख्या को सीमित करने वाली बाध्यता (6 अक्षर):

7 बाएँ से दाएँ: डिवाइस और सर्वर या नेटवर्क के बीच बना संपर्क, जिससे डेटा का आदान-प्रदान होता है (4 अक्षर):

ऊपर से नीचे

1 ऊपर से नीचे: वह देश या शहर, जहां वीपीएन सर्वर भौतिक रूप से स्थित है और जिससे आपका आईपी दिखता है (5 अक्षर):

3 ऊपर से नीचे: एक साथ कई डिवाइस जोड़ने वाली सदस्यता की सीमा (6 अक्षर):

6 ऊपर से नीचे: नियमित शुल्क पर मिलने वाली सेवा की सदस्यता, जैसे मासिक या वार्षिक योजना (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।

के	स	ट	मि	ट	सा	य	क	च	ऊ	नी	जी	इ	त	म
पे	इ	ब	प	जि	मी	ने	ने	स	ले	इ	सी	य	छ	र
दे	वा	कि	जा	सा	वा	ड	क्श	रे	ब्स	स	ख	नि	फ	ढ
मा	डि	ना	का	रे	दे	सि	न	मी	क	क्रि	पि	ता	ति	ज
श	स	भ	ऊ	अ	ए	ऊ	ए	रि	वि	सु	प्श	श	स	य
वि	द	व	वा	पा	ई	ल	पी	च	से	कि	र	न	र्व	य
मा	घ	प	के	की	ए	व	सि	य	री	त	की	क्षा	र	कि
सी	सि	ना	ने	पा	स	ते	ण	ए	र	ता	सा	मी	स्था	न
स	नी	ऋ	ले	घ	ए	ति	जि	ला	ए	टू	जी	ले	न	ड
इ	ल	द	जे	घ	न्क्रि	के	च	से	दे	री	पी	ए	पी	उ
वा	अ	जे	मि	घ	प्श	व	आ	च	मी	च	ट	य	थ	फ
डि	ग	ना	सी	का	न	ज	फ	नी	जी	ता	ठ	से	र	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
प	कि	से	य	ह	ह	ते	रा	द	सा	सी	थ	जे	इ	मे

शब्दावली शब्द-सूची

एईएसएन्क्रिप्शन दसडिवाइस पीयरटूपीयर सुरक्षा कनेक्शन सब्सक्रिप्शन सर्वरस्थान डिवाइससीमा

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. एईएसएन्क्रिप्शन**
- **B. दसडिवाइस**
- **C. पीयरटूपीयर**
- **D. सुरक्षा**
- **E. कनेक्शन**
- **F. सब्सक्रिप्शन**
- **G. सर्वरस्थान**
- **H. डिवाइससीमा**

परिभाषाएँ और मिलान फ़ील्ड

1. नियमित शुल्क पर मिलने वाली सेवा की सदस्यता, जैसे मासिक या वार्षिक योजना।
2. औद्योगिक स्तर का एन्क्रिप्शन मानक।
3. ऑनलाइन डेटा और पहचान को खतरों तथा अनधिकृत पहुंच से बचाए रखने की स्थिति।
4. एक साथ कई डिवाइस जोड़ने वाली सदस्यता की सीमा।
5. फ़ाइल साझा करने के लिए समर्पित सर्वर श्रेणियां।
6. वह देश या शहर, जहां वीपीएन सर्वर भौतिक रूप से स्थित है और जिससे आपका आईपी दिखता है।
7. सक्रिय डिवाइस सत्रों की संख्या को सीमित करने वाली बाध्यता।
8. डिवाइस और सर्वर या नेटवर्क के बीच बना संपर्क, जिससे डेटा का आदान-प्रदान होता है।

चेकपॉइंट 7: उलझे शब्दों की चुनौती

नीचे के अक्षरों को सुलझाकर इस वर्कशीट की प्रमुख अवधारणाएँ पता करें। अपने उत्तर दिए गए इनपुट बॉक्स में लिखें।

1. प्श स ए ए न्क्रि ई न ए
2. पी र र य पी टू य
3. न क क्श ने
4. र न स्था स र्व
5. वा डि स द इ स
6. र क्षा सु
7. प्श न स क्रि ब्स
8. इ मा डि सी स वा

अतिरिक्त गतिविधि: झटपट सोचें

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

1	आपका VPN कनेक्शन धीमा होने के संकेत			
2	इस वर्कशीट में आपके सीखे हुए सुरक्षा शब्द			
3	ऐसी चीज़ें जिन्हें Avast SecureLine आपके नेटवर्क से छिपा सकता है			
4	एक अच्छे VPN ऐप का वर्णन करने वाले शब्द			
5	ऐसे डिवाइस जिन पर आप Avast SecureLine इंस्टॉल करेंगे			
6	ऐसे देश जहाँ आप Avast SecureLine सर्वर चाहेंगे			
7	आपके जाने-पहचाने VPN प्रोटोकॉल			
8	स्ट्रीमिंग सेवाएँ जो आप देखते हैं			
9	ऐसी स्थितियाँ जिनमें किल स्विच मददगार होता है			
10	ऐसी जगहें जहाँ आप Avast SecureLine चालू करेंगे			
11	ऐसे ऐप जिन्हें आप Avast SecureLine के साथ इस्तेमाल करेंगे			
12	ऐसा डेटा जिसे VPN को कभी स्टोर नहीं करना चाहिए			
13	VPN ऐप के बटन या मेनू			
14	ऐसी चीज़ें जो आप रोज़ ऑनलाइन करते हैं			
15	Avast SecureLine चुनने के कारण			

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: लॉगिंग अनुपालन



परिदृश्य: एक उपयोगकर्ता Avast की लॉगिंग नीति देखता है और पाता है कि ब्राउज़िंग डेटा स्टोर नहीं होता, लेकिन Avast क्षमता नियोजन के लिए कनेक्शन की अवधि और कच्चा बैंडविड्थ उपयोग रिकॉर्ड करता है।

चर्चा प्रश्न: इन्फ्रास्ट्रक्चर लोड की निगरानी के लिए Avast अस्थायी रूप से कौन-सा सेशन मीट्रिक लॉग करता है?

केस स्टडी 2: फ़ायरवॉल को बायपास करना



परिदृश्य: एक इंजीनियर पैकेट हेडर स्कैन करके OpenVPN ट्रैफ़िक ब्लॉक करने वाले नेटवर्क फ़ायरवॉल को बायपास करने की कोशिश करता है। उसे ऐसा प्रोटोकॉल चाहिए जो VPN पैकेट को सामान्य HTTPS डेटा के रूप में छिपा दे।

चर्चा प्रश्न: Avast SecureLine का कौन-सा प्रोटोकॉल विकल्प इस डीप पैकेट फ़िल्टरिंग से बचने के लिए बनाया गया 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

37	47	37	47	13		34	60	46	38	39	41	56	40		33	45	18	46	32

32	47	38	37	54	57		44	52		35	18	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: Avast SecureLine VPN क्या है?

Avast द्वारा विकसित सदस्यता-आधारित VPN सेवा, जो Avast इकोसिस्टम के भीतर सुरक्षा एकीकरण पर केंद्रित है।

Q2: Mimic प्रोटोकॉल क्या है?

Avast का मालिकाना कनेक्शन प्रोटोकॉल जो VPN हस्ताक्षर छिपाने और डीप पैकेट इंस्पेक्शन नियमों को बायपास करने के लिए बना है।

Q3: Avast VPN कहाँ स्थित है?

यह Prague, Czech Republic में स्थित है, जिससे यह EU के कानूनी और डेटा नियमों के अधीन आता है। [10]

Q4: क्या Avast SecureLine लॉग रखता है?

Avast के अनुसार वह आपके कनेक्ट और डिस्कनेक्ट होने का समय, सत्र की अवधि और उपयोग की गई बैंडविड्थ लॉग करता है, लेकिन आपकी देखी गई वेबसाइटें नहीं। [2]

Q5: Avast कौन-सा एन्क्रिप्शन मानक उपयोग करता है?

यह OpenVPN, WireGuard, IPsec (Mac) और Mimic प्रोटोकॉल के साथ AES-256 एन्क्रिप्शन का उपयोग 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 मैं Avast VPN से कई डिवाइस कनेक्ट कर सकता हूँ?

हाँ, Multi-Device प्लान एक साथ दस डिवाइस तक को कवर करता है (सितंबर 2026 तक)।

Q7: क्या Avast VPN P2P फ़ाइल शेयरिंग सपोर्ट करता है?

हाँ, Prague जैसे आठ निर्दिष्ट स्थानों के सर्वरों पर P2P और टोरेंटिंग की अनुमति है।

Q8: Avast Kill Switch की क्या भूमिका है?

VPN कनेक्शन टूटने पर यह सारा इंटरनेट एक्सेस ब्लॉक कर देता है, जिससे असुरक्षित डेटा लीक नहीं होता।

Q9: क्या Avast सार्वजनिक Wi-Fi कनेक्शन को सुरक्षित करता है?

हाँ, इसे ऐसे कॉन्फ़िगर किया जा सकता है कि असुरक्षित Wi-Fi नेटवर्क मिलते ही यह अपने-आप कनेक्ट हो जाए। [8]

Q10: Avast SecureLine के लिए रिफ़ंड अवधि क्या है?

Avast अपने VPN सब्सक्रिप्शन स्तरों पर मानक 30 दिन की मनी-बैक गारंटी देता है। [1]

चेकपॉइंट 10: उन्नत VPN FAQ (भाग C)

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

Q1: Mimic प्रोटोकॉल डीप पैकेट इंस्पेक्शन को कैसे बायपास करता है?

Avast बहुत कम तकनीकी विवरण प्रकाशित करता है; समीक्षक Mimic को VPN ट्रैफ़िक को सामान्य वेब डेटा जैसा दिखाने वाला बताते हैं।

Q2: चेक गणराज्य के क्षेत्राधिकार के क्या कानूनी निहितार्थ हैं?

चेकिया EU का सदस्य राज्य है, इसलिए GDPR तय करता है कि Avast अपने उपयोगकर्ताओं का व्यक्तिगत डेटा कैसे इकट्ठा करता और रखता है।

Q3: Avast कनेक्शन टाइमस्टैम्प क्यों लॉग करता है?

Avast सक्रिय डिवाइस सीमाएँ लागू करने और सर्वर क्षमता की सीमाओं की रीयल टाइम निगरानी के लिए कनेक्शन मेट्रिक्स का उपयोग करता है।

Q4: Avast SecureLine DNS लीक से कैसे बचाता है?

क्लाइंट सभी DNS लुकअप निजी Avast DNS सर्वरों से गुज़ारता है और स्थानीय ISP के नेटवर्क एडाप्टर की सेटिंग्स को अनदेखा कर देता है।

Q5: Mimic प्रोटोकॉल का स्पीड ओवरहेड कितना है?

Avast कोई आँकड़े प्रकाशित नहीं करता; अतिरिक्त ऑब्फ़स्केशन कुछ ओवरहेड जोड़ता है, इसलिए Mimic का उपयोग तब सबसे अच्छा है जब अन्य प्रोटोकॉल ब्लॉक हों।

चेकपॉइंट 10: उन्नत VPN FAQ (भाग D)

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

Q6: क्या मैं अपने राउटर पर Avast VPN सेट कर सकता हूँ?

राउटर सेटअप आधिकारिक रूप से समर्थित नहीं है; इसके बजाय Avast, Windows, Mac, Android और iOS के लिए ऐप देता है।

Q7: Avast का सिस्टम-स्तर का Kill Switch प्रतिस्पर्धियों के ऐप्स से कैसे अलग है?

VPN के दोबारा कनेक्ट होने तक यह सारा इंटरनेट एक्सेस ब्लॉक कर देता है, और स्थानीय प्रिंटर व शेयर तक पहुँचने का विकल्प भी रहता है। [7]

Q8: क्या Avast VPN स्प्लिट टनलिंग सपोर्ट करता है?

हाँ, स्प्लिट टनलिंग Android और Windows क्लाइंट पर समर्थित है, जिससे चुनिंदा ऐप्स एन्क्रिप्शन को बायपास कर सकते हैं।

Q9: Avast WebRTC लीक सुरक्षा कैसे संभालता है?

Avast में WebRTC की कोई विशेष सेटिंग दर्ज नहीं है, इसलिए अपनी ब्राउज़र सेटिंग में भी WebRTC लीक बंद करें।

Q10: चेक गणराज्य प्राथमिक Five Eyes गठबंधन से बाहर क्यों है?

Five Eyes में अमेरिका, ब्रिटेन, कनाडा, ऑस्ट्रेलिया और न्यूज़ीलैंड हैं; चेकिया EU में है, इस समझौते में नहीं।

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

Avast का मालिकाना Mimic प्रोटोकॉल उन देशों में VPN ब्लॉक को पार करने के लिए बना है जहाँ VPN के उपयोग पर रोक है। [9]

2. VPN इनसाइट

Avast VPN चेक गणराज्य में निगमित है, इसलिए यह यूरोपीय डेटा गोपनीयता नियमों के अधीन है।

3. VPN इनसाइट

Avast का Multi-Device प्लान एक खाते पर दस डिवाइस तक को कवर करता है (सितंबर 2026 तक)। [1]

4. VPN इनसाइट

Avast कनेक्शन की अवधि और बैंडविड्थ डेटा लॉग करता है, लेकिन देखे गए वेब डोमेन रिकॉर्ड नहीं करता। [2]

5. VPN इनसाइट

P2P फ़ाइल शेयरिंग Prague समेत आठ निर्धारित स्थानों के सर्वरों पर अनुमत है। [2]

6. VPN इनसाइट

Avast SecureLine AES-256 एन्क्रिप्शन का उपयोग करता है, जो गोपनीय सरकारी डेटा की सुरक्षा के लिए मान्य मानक है।

7. VPN इनसाइट

क्लाइंट में ऑटो-सिक्योर नियम हैं, जो सार्वजनिक Wi-Fi नेटवर्क पहचानते ही सुरक्षा चालू कर देते हैं।

8. VPN इनसाइट

DNS लीक सुरक्षा सभी नाम-समाधान क्वेरी को सुरक्षित, निजी Avast DNS सर्वरों से होकर जाने के लिए बाध्य करती है।

9. VPN इनसाइट

सभी नई SecureLine सदस्यता योजनाओं के लिए 30 दिन की मनी-बैक गारंटी दी जाती है। [1]

10. VPN इनसाइट

SecureLine भविष्य के क्वांटम हमलों से बचाव के लिए वैकल्पिक पोस्ट-क्वांटम एन्क्रिप्शन देता है। [2]

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] Avast. (n.d.). Avast SecureLine VPN Download | VPN Free Trial.
https://www.avast.com/secureline-vpn

[2] Avast Support. (n.d.). Avast SecureLine VPN - FAQs.
https://support.avast.com/en-en/article/secureline-vpn-faq/

[3] Avast Support. (n.d.). Avast SecureLine VPN for Windows and Mac - Getting Started.
https://support.avast.com/en-fi/article/use-secureline-vpn/

[4] Avast. (2026). Product Privacy Notice.
https://www.avast.com/products-policy

[5] SoftwareLab. (2025). Avast SecureLine VPN Review (2026).
https://softwarelab.org/avast-vpn-review/

[6] VPN.com. (2026). Avast SecureLine VPN Review: Features & Performance.
https://www.vpn.com/vpn/avast-secureline-vpn/

[7] Avast. (n.d.). Avast SecureLine VPN for Windows and Mac - Getting Started.
https://support.avast.com/en-us/article/152/

[8] Avast. (n.d.). Managing connection rules in Avast SecureLine VPN for Android.
https://support.avast.com/en-us/article/android-secureline-vpn-connection-rules/

[9] Avast. (n.d.). Troubleshooting common issues with Avast SecureLine VPN.
https://support.avast.com/en-us/article/troubleshoot-secureline-vpn/

[10] Office for Personal Data Protection (Czech Republic). (2024). Czech DPA imposed fine of 351 million CZK for GDPR infringement.
https://uoou.gov.cz/en/news/business-communication/czech-dpa-imposed-fine-of-351-million-czk-for-gdpr-infringement

[11] European Commission. (n.d.). Legal framework of EU data protection.
https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en

उत्तर कुंजी: चेकपॉइंट 1 – बहुविकल्पीय

1 **प्रश्न 1** सही उत्तर: A

शिक्षण नोट

Mimic, Avast का अपना प्रोटोकॉल है, जो उन जगहों पर VPN ब्लॉक से बचने के लिए बनाया गया है जहाँ मानक प्रोटोकॉल प्रतिबंधित हैं।

2 **प्रश्न 2** सही उत्तर: A

शिक्षण नोट

Avast का मुख्यालय प्राग, चेक गणराज्य में है।

3 **AES-256 शील्ड** AES-256 सही उत्तर: A

शिक्षण नोट

AES-256 गोपनीय डेटा को सुरक्षित करने के लिए मानक स्वीकृत एल्गोरिदम है। संदर्भ: AES Standard।

4 **डिवाइस लिंक** दस डिवाइस सही उत्तर: A

शिक्षण नोट

Avast का multi-device प्लान एक साथ दस डिवाइस लिंक कनेक्शन तक की अनुमति देता है। उद्धरण: Subscription Terms। [2]

5 **प्रश्न 5** सही उत्तर: A

शिक्षण नोट

Avast की नीति के अनुसार वह कनेक्शन समय, अवधि और बैंडविड्थ लॉग करता है, लेकिन देखी गई साइटें नहीं।

उत्तर कुंजी: चेकपॉइंट 2 – सही या गलत

6 **Mimic प्रोटोकॉल** Mimic बाईपास

सही उत्तर: सही

शिक्षण नोट

Mimic प्रोटोकॉल कनेक्शन पैकेट को लपेटकर नेटवर्क फ़ायरवॉल फ़िल्टर से बच निकलता है। संदर्भ: Mimic Spec।

7 **प्रश्न 7**

सही उत्तर: गलत

शिक्षण नोट

गलत: Avast कनेक्शन मेटाडेटा रखता है, और उसके VPN का कभी स्वतंत्र ऑडिट नहीं हुआ है।

8 **प्रश्न 8**

सही उत्तर: सही

शिक्षण नोट

सही: Avast आठ निर्धारित लोकेशन के सर्वरों पर P2P ट्रैफ़िक की अनुमति देता है।

9 **प्रश्न 9**

सही उत्तर: गलत

शिक्षण नोट

गलत: चेकिया EU का सदस्य है, इसलिए GDPR जैसा EU डेटा कानून Avast पर लागू होता है।

10 **प्रश्न 10**

सही उत्तर: सही

शिक्षण नोट

सही: Avast का Kill Switch Windows, Mac और Android 8.0 या उसके बाद के संस्करण पर उपलब्ध है। [2]

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. Mimic	F 2. चेक गणराज्य	B 3. AES-256	E 4. दस डिवाइस
G 5. टाइमस्टैम्प	C 6. KILL SWITCH	H 7. पीयर-टू-पीयर	A 8. ओवरहेड

चेकपॉइंट 3: उत्तर – प्रमुख शब्द

1 सुरक्षा	2 सर्वर स्थान	3 एईएस एन्क्रिप्शन	4 दस डिवाइस
5 कनेक्शन	6 डिवाइस सीमा		

चेकपॉइंट 6, वैकल्पिक: उत्तर – शब्द मिलान

1 F – सब्सक्रिप्शन	2 A – एईएसएन्क्रिप्शन	3 D – सुरक्षा	4 B – दसडिवाइस
5 C – पीयरटूपीयर	6 G – सर्वरस्थान	7 H – डिवाइससीमा	8 E – कनेक्शन

शिक्षकों के लिए चर्चा नोट

प्रमुख शब्द:
जाँचें कि क्या विद्यार्थी Mimic, चेक गणराज्य और AES-256 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

के	स	ट	मि	ट	सा	य	क	च	ऊ	नी	जी	इ	त	म
पे	इ	ब	प	जि	मी	ने	ने	स	ले	इ	सी	य	छ	र
दे	वा	कि	जा	सा	वा	ड	क्श	रे	ब्स	स	ख	नि	फ	ढ
मा	डि	ना	का	रे	दे	सि	न	मी	क	क्रि	पि	ता	ति	ज
श	स	भ	ऊ	अ	ए	ऊ	ए	रि	वि	सु	प्श	श	स	य
वि	द	व	वा	पा	ई	ल	पी	च	से	कि	र	न	र्व	य
मा	घ	प	के	की	ए	व	सि	य	री	त	की	क्षा	र	कि
सी	सि	ना	ने	पा	स	ते	ण	ए	र	ता	सा	मी	स्था	न
स	नी	ऋ	ले	घ	ए	ति	जि	ला	ए	ट्ट	जी	ले	न	ड
इ	ल	द	जे	घ	क्रि	के	च	से	दे	री	पी	ए	पी	उ
वा	अ	जे	मि	घ	प्श	व	आ	च	मी	च	ट	य	थ	फ
डि	ग	ना	सी	का	न	ज	फ	नी	जी	ता	ठ	से	र	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
प	कि	से	य	ह	ह	ते	रा	द	सा	सी	थ	जे	इ	मे

क्रॉसवर्ड समाधान



क्रॉसवर्ड समाधान के लिए शिक्षक गाइड

बाएँ से दाएँ

2 बाएँ से दाएँ: सुरक्षा ऑनलाइन डेटा और पहचान को खतरों तथा अनधिकृत पहुंच से बचाए रखने की स्थिति (3 अक्षर)

4 बाएँ से दाएँ: एईएसएन्क्रिप्शन औद्योगिक स्तर का एन्क्रिप्शन मानक (8 अक्षर)

5 बाएँ से दाएँ: डिवाइससीमा सक्रिय डिवाइस सत्रों की संख्या को सीमित करने वाली बाध्यता (6 अक्षर)

7 बाएँ से दाएँ: कनेक्शन डिवाइस और सर्वर या नेटवर्क के बीच बना संपर्क, जिससे डेटा का आदान-प्रदान होता है (4 अक्षर)

ऊपर से नीचे

1 ऊपर से नीचे: सर्वरस्थान वह देश या शहर, जहां वीपीएन सर्वर भौतिक रूप से स्थित है और जिससे आपका आईपी दिखता है (5 अक्षर)

3 ऊपर से नीचे: दसडिवाइस एक साथ कई डिवाइस जोड़ने वाली सदस्यता की सीमा (6 अक्षर)

6 ऊपर से नीचे: सब्सक्रिप्शन नियमित शुल्क पर मिलने वाली सेवा की सदस्यता, जैसे मासिक या वार्षिक योजना (5 अक्षर)

अक्षर-फेर शब्द और कूट संदेश हल कुंजी

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

शब्द अनस्क्रैम्बल कुंजी

1. प्श स ए ए न्क्रि ई न ए — **एईएसएएन्क्रिप्शन**
2. पी र र य पी ट्ट य — **पीयरट्टूपीयर**
3. न क क्श ने — **कनेक्शन**
4. र न स्था स र्व — **सर्वरस्थान**
5. वा डि स द इ स — **दसडिवाइस**
6. र क्षा सु — **सुरक्षा**
7. प्श न स क्रि ब्स — **सब्सक्रिप्शन**
8. इ मा डि सी स वा — **डिवाइससीमा**

गुप्त कूट चुनौती कुंजी

"मिमिक फ़ायरवॉल पहचान नियमों से बचाता"

केस स्टडी के उत्तर

A केस स्टडी 1: लॉगिंग अनुपालन

शिक्षक समाधान

ग्रेडिंग दिशानिर्देश

छात्रों के उत्तरों में निम्नलिखित बिंदु शामिल होने चाहिए:

- परिदृश्य विश्लेषण: एक उपयोगकर्ता Avast की लॉगिंग नीति देखता है और पाता है कि ब्राउज़िंग डेटा सहेजा नहीं जाता, लेकिन क्षमता नियोजन के लिए Avast कनेक्शन की अवधि और रॉ बैंडविड्थ उपयोग दर्ज करता है।
- अनुशंसित रणनीति और समाधान: Avast क्षमता प्रबंधन के लिए सक्रिय सेशन के दौरान कनेक्शन टाइमस्टैम्प और रॉ डेटा वॉल्यूम रिकॉर्ड करता है।

B केस स्टडी 2: फ़ायरवॉल को बायपास करना

शिक्षक समाधान

ग्रेडिंग दिशानिर्देश

छात्रों के उत्तरों में निम्नलिखित बिंदु शामिल होने चाहिए:

- परिदृश्य विश्लेषण: एक इंजीनियर पैकेट हेडर स्कैन करके OpenVPN ट्रैफ़िक को ब्लॉक करने वाले नेटवर्क फ़ायरवॉल को बायपास करने की कोशिश करता है। उसे ऐसा प्रोटोकॉल चाहिए जो VPN पैकेट को सामान्य HTTPS डेटा जैसा दिखा दे।
- अनुशंसित रणनीति और समाधान: इंजीनियर को Mimic प्रोटोकॉल कॉन्फ़िगर करना चाहिए, जो VPN पैकेट को लपेटकर और ढककर उन्हें सामान्य सुरक्षित ब्राउज़र अनुरोधों जैसा बना देता है।