नाम: _____ दिनांक: _____ अंक: _____

Private Internet Access समीक्षा

Private Internet Access VPN का तकनीकी विश्लेषण, ओपन-सोर्स डेस्कटॉप और मोबाइल क्लाइंट कोडबेस, अदालत में सिद्ध ज़ीरो-लॉग, पोर्ट फ़ॉरवर्डिंग और PIA MACE विज्ञापन फ़िल्टरिंग।

PRIVATE INTERNET ACCESS 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 Private Internet Access की तकनीकी समीक्षा से परिचित कराता है। आप ओपन-सोर्स डेस्कटॉप क्लाइंट, अदालत में सिद्ध ज़ीरो लॉग, पोर्ट फ़ॉरवर्डिंग और PIA MACE विज्ञापन ब्लॉकिंग 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/pia/

आपका Private Internet Access लर्निंग रोडमैप

- Private Internet Access 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।

PRIVATE INTERNET ACCESS समीक्षा 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 अदालत में सिद्ध लॉगिंग और PIA MACE पर लागू करें। अंत में अतिरिक्त गतिविधि झटपट सोचें पूरी करें।

अदालत में प्रमाणित ज़ीरो लॉग्स और ओपन-सोर्स डेस्कटॉप क्लाइंट (परिचय)

Private Internet Access (PIA) का क्लाइंट कोडबेस अत्यधिक अनुकूलन योग्य और ओपन-सोर्स है। उसने अमेरिकी अदालतों में अपनी ज़ीरो-लॉग प्रतिबद्धताएँ साबित की हैं और पोर्ट फ़ॉरवर्डिंग तथा MACE विज्ञापन ब्लॉकिंग जैसे उन्नत कॉन्फ़िगरेशन को एकीकृत करता है।

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

चेकपॉइंट 1: बहुविकल्पीय चुनौती

1. Private Internet Access VPN का व्यावसायिक नाम क्या है?
   - A) PIA VPN
   - B) Safe Connect
   - C) Threat Protection
   - D) Proton VPN

2. Private Internet Access का मुख्यालय किस देश में है, जिससे वह अमेरिकी कानूनों के अधीन है?
   - A) संयुक्त राज्य अमेरिका
   - B) यूनाइटेड किंगडम
   - C) रोमानिया
   - D) स्विट्ज़रलैंड

3. PIA अपने डेस्कटॉप क्लाइंट में कौन-सा स्वामित्व वाला विज्ञापन-ब्लॉकिंग टूल शामिल करता है?
   - A) PIA MACE
   - B) Threat Protection
   - C) Safe Shield
   - D) CleanWeb

4. मानक PIA अकाउंट के तहत एक साथ डिवाइस कनेक्शन की सीमा क्या है?
   - A) असीमित
   - B) पाँच डिवाइस
   - C) दस डिवाइस
   - D) सात डिवाइस

5. OpenVPN के अलावा PIA ऐप्स कौन-सा आधुनिक ओपन-सोर्स प्रोटोकॉल इस्तेमाल कर सकते हैं?
   - A) WireGuard
   - B) PPTP
   - C) SSTP
   - D) L2TP

चेकपॉइंट 2: सही या गलत चुनौती

6 प्रश्न 6

6. Private Internet Access का मुख्यालय अमेरिका में है और वह Five Eyes क्षेत्राधिकार के अधीन है।

○ सही ○ गलत

7 प्रश्न 7

7. PIA ने अमेरिकी संघीय अदालत के सम्मनों में अपनी ज़ीरो-लॉग नीति साबित की है।

○ सही ○ गलत

8 प्रश्न 8

8. PIA MACE विज्ञापन ब्लॉकिंग DNS अनुरोधों को फ़िल्टर करके क्लाइंट के भीतर काम करती है।

○ सही ○ गलत

9 प्रश्न 9

9. PIA मैनुअल पोर्ट फ़ॉरवर्डिंग कॉन्फ़िगरेशन को सपोर्ट नहीं करता।

○ सही ○ गलत

10 प्रश्न 10

10. सभी PIA डेस्कटॉप क्लाइंट एप्लिकेशन पूरी तरह ओपन-सोर्स 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. PIA का स्टैंडअलोन क्लाइंट एक ऐसा _____ है, जिसे आप अपने कंप्यूटर पर इंस्टॉल करते हैं।
2. अमेरिकी अधिकारिता होने पर भी PIA उपयोगकर्ता डेटा के _____ पर ज़ोर देता है।
3. नेटवर्क में अनचाहे प्रवेश को रोकने वाला _____ PIA के साथ मिलकर सुरक्षा बढ़ाता है।
4. सब्सक्राइबर _____ समवर्ती लाइसेंस के साथ बहुत बड़ी संख्या में डिवाइस जोड़ सकते हैं।
5. PIA ऐप OpenVPN की जगह तेज़, आधुनिक _____ प्रोटोकॉल का उपयोग कर सकते हैं।
6. ज़ीरो-लॉग्स नीति संघीय अदालत के सम्मनों में _____ होकर सत्यापित हुई है।

शब्दावली शब्द-बैंक

अदालत प्रमाणित असीमित प्रमाणीकरण फ़ायरवॉल वायरगार्ड संरक्षण सॉफ़्टवेयर हार्डवेयर

अपने उत्तर यहाँ लिखें:

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

चेकपॉइंट 4: VPN और नेटवर्क अवधारणा मिलान

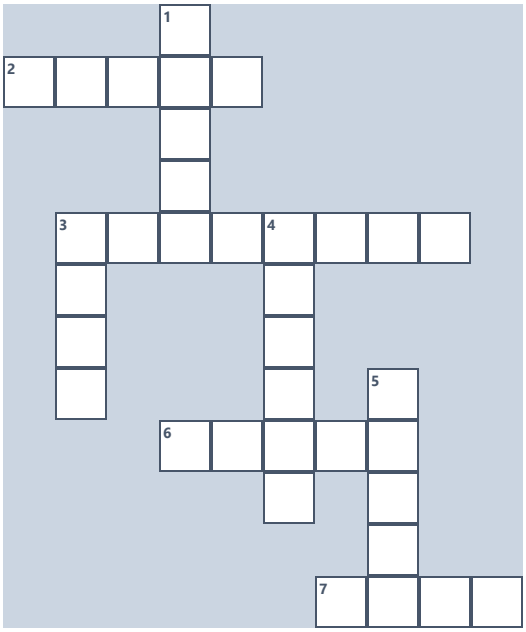
परिभाषा मिलान

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. PIA VPN**	**A**	नेटवर्क पार करने के लिए पैकेट पेलोड को एनकैप्सुलेट करना।
☐	**2. संयुक्त राज्य अमेरिका**	**B**	क्लाइंट में बना DNS-आधारित विज्ञापन और ट्रैकर ब्लॉकर।
☐	**3. PIA MACE**	**C**	आधुनिक, तेज़ गति वाला ओपन-सोर्स कनेक्शन प्रोटोकॉल।
☐	**4. असीमित**	**D**	फ़ेलसेफ़ ब्लॉकर जो टनल ड्रॉप होने पर ट्रैफ़िक काट देता है।
☐	**5. WireGuard**	**E**	कानूनी अनुरोधों से मान्य की गई लॉग नीति, जिनमें कोई डेटा नहीं मिला।
☐	**6. अदालत में प्रमाणित**	**F**	उत्तरी अमेरिकी कानूनी क्षेत्राधिकार और कॉर्पोरेट मुख्यालय।
☐	**7. Kill Switch**	**G**	बिना सीमा वाली एक साथ डिवाइस कनेक्शन नीति।
☐	**8. टनलिंग**	**H**	Private Internet Access का व्यावसायिक ब्रांड वाला स्टैंडअलोन क्लाइंट।

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. कंप्यूटर या फ़ोन पर चलने वाले प्रोग्रामों का समूह (5)

3. कानूनी अनुरोधों से सत्यापित लॉग नीति, जिनसे कोई डेटा नहीं मिला (8)

6. आधुनिक, उच्च-गति वाला ओपन-सोर्स कनेक्शन प्रोटोकॉल (5)

7. किसी चीज़ को नुकसान और ख़तरे से बचाकर रखना (4)

ऊपर से नीचे

1. अनचाहे नेटवर्क ट्रैफ़िक को रोकने वाली सुरक्षा दीवार (5)

3. बिना सीमा की समवर्ती डिवाइस कनेक्शन नीति (4)

4. पासवर्ड या कोड से साबित करना कि उपयोगकर्ता वही है जो वह कहता है (6)

5. कंप्यूटर या सर्वर के भौतिक पुर्ज़े और मशीनें (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: कंप्यूटर या फ़ोन पर चलने वाले प्रोग्रामों का समूह (5 अक्षर):

3 बाएँ से दाएँ: कानूनी अनुरोधों से सत्यापित लॉग नीति, जिनसे कोई डेटा नहीं मिला (8 अक्षर):

6 बाएँ से दाएँ: आधुनिक, उच्च-गति वाला ओपन-सोर्स कनेक्शन प्रोटोकॉल (5 अक्षर):

7 बाएँ से दाएँ: किसी चीज़ को नुकसान और ख़तरे से बचाकर रखना (4 अक्षर):

ऊपर से नीचे

1 ऊपर से नीचे: अनचाहे नेटवर्क ट्रैफ़िक को रोकने वाली सुरक्षा दीवार (5 अक्षर):

3 ऊपर से नीचे: बिना सीमा की समवर्ती डिवाइस कनेक्शन नीति (4 अक्षर):

4 ऊपर से नीचे: पासवर्ड या कोड से साबित करना कि उपयोगकर्ता वही है जो वह कहता है (6 अक्षर):

5 ऊपर से नीचे: कंप्यूटर या सर्वर के भौतिक पुर्ज़े और मशीनें (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	ल	रि	द	जे	घ	छ	ई	के
द	र्ड	प	ति	के	ट	मि	ट	सॉ	सा	य	च	ऊ	नी	जी
इ	गा	त	म	पे	ब	प	जि	मी	फ़्ट	ने	ले	इ	सी	य
छ	र	र	दे	कि	जा	सा	वा	ड	रे	वे	स	ख	नि	फ
ढ	य	मा	ना	का	अ	रे	दे	सि	मी	क	य	पि	अ	ता
ति	वा	ज	श	भ	दा	ऊ	प्र	अ	ऊ	ए	रि	र	सी	वि
ण	क्ष	र	सं	श	ल	य	वि	मा	व	वा	पा	ल	मि	च
ल	से	कि	य	घ	त	प	के	की	णी	व	सि	री	त	त
वॉ	की	कि	सि	ना	प्र	ने	पा	ते	ण	क	ए	ता	सा	मी
र	न	नी	ऋ	ले	मा	घ	ति	जि	ला	ए	र	जी	ले	ड
य	ल	द	जे	घ	णि	के	च	से	दे	री	ए	ण	पी	हा
फ़ा	उ	अ	जे	मि	त	घ	व	आ	च	मी	च	ट	र्ड	थ
फ	ग	ना	सी	का	ज	फ	नी	जी	ता	ठ	से	वे	लि	ट
आ	इ	से	रा	के	री	पा	वा	सि	य	नि	य	पि	ने	ख
के	वे	ऊ	ड	नी	दे	दि	भ	आ	नि	र	जे	वे	वे	ष

शब्दावली शब्द-सूची

असीमित, वायरगार्ड, अदालतप्रमाणित, फ़ायरवॉल संरक्षण, सॉफ़्टवेयर, हार्डवेयर, प्रमाणीकरण

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. असीमित**
- **B. वायरगार्ड**
- **C. अदालतप्रमाणित**
- **D. फ़ायरवॉल**
- **E. सॉफ़्टवेयर**
- **F. हार्डवेयर**
- **G. प्रमाणीकरण**
- **H. संरक्षण**

परिभाषाएँ और मिलान फ़ील्ड

1. कानूनी अनुरोधों से सत्यापित लॉग नीति, जिनसे कोई डेटा नहीं मिला।
2. कंप्यूटर या सर्वर के भौतिक पुर्ज़े और मशीनें।
3. किसी चीज़ को नुकसान और ख़तरे से बचाकर रखना।
4. पासवर्ड या कोड से साबित करना कि उपयोगकर्ता वही है जो वह कहता है।
5. आधुनिक, उच्च-गति वाला ओपन-सोर्स कनेक्शन प्रोटोकॉल।
6. अनचाहे नेटवर्क ट्रैफ़िक को रोकने वाली सुरक्षा दीवार।
7. कंप्यूटर या फ़ोन पर चलने वाले प्रोग्रामों का समूह।
8. बिना सीमा की समवर्ती डिवाइस कनेक्शन नीति।

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. मि अ त सी
2. त अ त दा णि मा प्र ल
3. वे सॉ र य फ़्ट
4. ण क णी र प्र मा
5. र र्ड वा गा य
6. वॉ फ़ा र ल य
7. य र हा वे र्ड
8. सं ण क्ष र

अतिरिक्त गतिविधि: झटपट सोचें

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

1	ऐसी स्थितियाँ जिनमें किल स्विच मददगार होता है			
2	एक अच्छे VPN ऐप का वर्णन करने वाले शब्द			
3	VPN ऐप के बटन या मेनू			
4	PIA में आप जिन सुविधाओं को देखते हैं			
5	PIA चुनने के कारण			
6	आपका VPN कनेक्शन धीमा होने के संकेत			
7	ऐसी जगहें जहाँ आप PIA चालू करेंगे			
8	ऐसे लोग जिन्हें आप PIA की सलाह देंगे			
9	ऐसा डेटा जिसे VPN को कभी स्टोर नहीं करना चाहिए			
10	ऐसे देश जहाँ आप PIA सर्वर चाहेंगे			
11	ऐसी चीज़ें जो आप रोज़ ऑनलाइन करते हैं			
12	PIA के अलावा अन्य VPN सेवाएँ			
13	VPN खरीदने से पहले जाँचने वाली चीज़ें			
14	ऐसी चीज़ें जिन्हें PIA आपके नेटवर्क से छिपा सकता है			
15	PIA कस्टमर सपोर्ट के लिए सवाल			

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: अदालत में प्रमाणित ज़ीरो लॉग्स का सत्यापन



परिदृश्य: एक सरकारी एजेंसी साइबर अपराध जाँच के दौरान किसी विशिष्ट IP एड्रेस के कनेक्शन लॉग माँगते हुए PIA को सम्मन जारी करती है।

चर्चा प्रश्न: विस्तार से बताइए कि PIA का सर्वर कॉन्फ़िगरेशन और ज़ीरो-लॉग्स आर्किटेक्चर उपयोगकर्ता डेटा उजागर किए बिना उसे सम्मन का पालन करने की अनुमति कैसे देते हैं।

केस स्टडी 2: कस्टम पोर्ट फ़ॉरवर्डिंग कॉन्फ़िगर करना



परिदृश्य: एक सॉफ़्टवेयर इंजीनियर एक अस्थायी लोकल सर्विस होस्ट करके उसे सुरक्षित VPN पोर्ट आवंटन के ज़रिए रिमोट टेस्टरों के साथ साझा करना चाहता है।

चर्चा प्रश्न: समझाइए कि PIA क्लाइंट में पोर्ट फ़ॉरवर्डिंग कैसे चालू की जाती है और कस्टम इनकमिंग पोर्ट उजागर करने के सुरक्षा समझौतों का विश्लेषण 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

33	47	38	46		41	48	33	48	8	32		44	49	39	13	61	43	46

11	39		15	54	33	32	48	38	28	46		30	52	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: Private Internet Access क्या है?

यह अत्यंत अनुकूलन योग्य, ओपन-सोर्स VPN प्रदाता है जो गति, सुरक्षा और डिजिटल गोपनीयता पर केंद्रित है।

Q2: PIA का मुख्यालय कहाँ है?

PIA का मुख्यालय Denver, Colorado में है और वह अमेरिकी क्षेत्राधिकार में काम करता है। [6]

Q3: क्या PIA लॉग रखता है?

नहीं, PIA सख़्त ज़ीरो-लॉग्स नीति लागू करता है, जिसका ऑडिट हुआ है और जिसे अदालत में कई बार सही साबित किया जा चुका है।

Q4: मैं कितने डिवाइस कनेक्ट कर सकता हूँ?

PIA एक ही सदस्यता प्लान में असीमित एक साथ डिवाइस कनेक्शन देता है। [1]

Q5: PIA MACE क्या है?

यह DNS-आधारित विज्ञापन, ट्रैकर और मैलवेयर ब्लॉकर है जो सीधे PIA क्लाइंट एप्लिकेशन में बना है।

चेकपॉइंट 10: बुनियादी VPN FAQ (भाग B)

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

Q6: क्या PIA WireGuard सपोर्ट करता है?

हाँ, ऐप्स में सेटिंग के Protocols सेक्शन में आप WireGuard या OpenVPN चुन सकते हैं।

Q7: क्या ऐप पोर्ट फ़ॉरवर्डिंग सपोर्ट करता है?

हाँ, PIA चुनिंदा सर्वरों पर बिल्ट-इन पोर्ट फ़ॉरवर्डिंग देता है, जिसे ऐप की Network सेटिंग्स में चालू किया जाता है।

Q8: क्या क्लाइंट ऐप्स ओपन-सोर्स हैं?

हाँ, सभी PIA डेस्कटॉप और मोबाइल क्लाइंट ऐप्लिकेशन पूरी तरह ओपन-सोर्स हैं और GitHub पर होस्ट किए गए हैं।

Q9: क्या इसमें किल स्विच है?

हाँ, इसमें एक उन्नत किल स्विच है जो VPN टनल गिरने पर सारा ट्रैफ़िक ब्लॉक कर देता है।

Q10: क्या मैं राउटर पर PIA इंस्टॉल कर सकता हूँ?

हाँ, PIA संगत राउटरों के लिए मैन्युअल OpenVPN और WireGuard कॉन्फ़िगरेशन देता है।

चेकपॉइंट 10: उन्नत VPN FAQ (भाग C)

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

Q1: ज़ीरो-लॉग नीति अदालत में कैसे साबित हुई है?

कई मौकों पर अमेरिकी संघीय सम्मनों में PIA से उपयोगकर्ताओं का कनेक्शन इतिहास माँगा गया, लेकिन ज़ीरो लॉगिंग के कारण कंपनी ने कोई डेटा नहीं दिया।

Q2: PIA MACE ब्राउज़र विज्ञापन-ब्लॉकर से कैसे अलग है?

MACE DNS स्तर पर काम करता है और विज्ञापन डोमेन के लिए खाली उत्तर लौटाता है, लेकिन पेज के तत्व छिपा नहीं सकता और गैर-DNS विज्ञापन स्ट्रीम को फ़िल्टर नहीं कर सकता।

Q3: PIA में WireGuard के लिए डिफ़ॉल्ट एन्क्रिप्शन मानक क्या है?

यह ChaCha20-Poly1305 सममित कुंजी एन्क्रिप्शन का उपयोग करता है, जो मोबाइल CPU पर AES-GCM से तेज़ है।

Q4: पोर्ट फ़ॉरवर्डिंग सुरक्षित रूप से कैसे कॉन्फ़िगर की जाती है?

क्लाइंट VPN गेटवे से एक खुला पोर्ट माँगता है, जिसे गेटवे आने वाले ट्रैफ़िक के लिए गतिशील रूप से मैप करता है और क्लाइंट के स्थानीय पोर्ट छिपाए रखता है।

Q5: PIA के लिए US के अधिकार क्षेत्र के जोखिम क्या हैं?

अमेरिका Five Eyes का सदस्य है; फिर भी, PIA कोई लॉग नहीं रखता, इसलिए सबपीना कंपनी को ऐसा डेटा देने के लिए बाध्य नहीं कर सकते जो मौजूद ही नहीं है।

चेकपॉइंट 10: उन्नत VPN FAQ (भाग D)

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

Q6: क्या PIA स्प्लिट टनलिंग सपोर्ट करता है?

हाँ, Split Tunnel नियम चुनिंदा ऐप्स या IP पतों को VPN बायपास करने या केवल उसी का उपयोग करने देते हैं।

Q7: Advanced Kill Switch कैसे काम करता है?

VPN क्लाइंट ऐप बंद होने पर भी यह सारा आउटबाउंड इंटरनेट एक्सेस ब्लॉक रखता है, जिससे कोई आकस्मिक लीक नहीं होता। [2]

Q8: क्या PIA shadowsocks ऑब्फ़स्केशन सपोर्ट करता है?

हाँ, यह सेंसर किए गए नेटवर्क में VPN ट्रैफ़िक के सिग्नेचर छिपाने के लिए Shadowsocks प्रॉक्सी के साथ मल्टी-हॉप रूटिंग की अनुमति देता है। [4]

Q9: PIA किस प्रकार के सर्वर चलाता है?

PIA का कहना है कि उसका नेटवर्क RAM-only सर्वरों पर चलता है, जो उपयोगकर्ता डेटा हार्ड ड्राइव पर नहीं लिख सकते क्योंकि उनमें हार्ड ड्राइव होती ही नहीं।

Q10: क्या क्लाइंट कस्टम MTU आकार को सपोर्ट करता है?

हाँ, उन्नत सेटिंग्स उपयोगकर्ताओं को प्रतिबंधित नेटवर्क पर कनेक्शन टूटने की समस्या सुलझाने के लिए MTU पैकेट समायोजित करने देती हैं।

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

Private Internet Access की स्थापना 2010 में London Trust Media ने की थी और 2019 में Kape Technologies ने उसे अधिग्रहित किया। [7]

2. VPN इनसाइट

PIA का कहना है कि उसकी नो-लॉग नीति की अमेरिकी अदालत में एक से अधिक बार परीक्षा हो चुकी है, जिनमें FBI से जुड़े मामले भी शामिल हैं। [1]

3. VPN इनसाइट

MACE विज्ञापनों, ट्रैकर और मैलवेयर के लिए इस्तेमाल होने वाले डोमेन को DNS स्तर पर, उनके लोड होने से पहले ही ब्लॉक कर देता है। [2]

4. VPN इनसाइट

PIA का कहना है कि वह 91 देशों में 10-Gbps नेटवर्क पर RAM-only सर्वर चलाता है (सितंबर 2026 तक)। [1]

5. VPN इनसाइट

सभी डेस्कटॉप और मोबाइल क्लाइंट ओपन-सोर्स हैं, जिससे कोई भी GitHub पर उनके सुरक्षा कॉन्फ़िगरेशन की जाँच कर सकता है। [8]

6. VPN इनसाइट

उन्नत स्प्लिट टनलिंग सुविधा स्थानीय ऐप्स के साथ-साथ गंतव्य IP रेंज के आधार पर भी ट्रैफ़िक रूट करने में सक्षम है। [2]

7. VPN इनसाइट

PIA का कॉर्पोरेट कार्यालय Denver, Colorado में है, जिससे कंपनी अमेरिकी कानून के अधीन आती है। [6]

8. VPN इनसाइट

Deloitte Audit Romania ने PIA की नो-लॉग्स व्यवस्था का ऑडिट किया और निष्कर्ष निकाला कि वह ऐसा कोई डेटा नहीं रखती जो उपयोगकर्ताओं या गतिविधि की पहचान करे। [1]

9. VPN इनसाइट

Advanced Kill Switch VPN बंद होने पर भी VPN के बाहर का सारा ट्रैफ़िक रोक देता है। [2]

10. VPN इनसाइट

यह उन उपयोगकर्ताओं के लिए ऐड-ऑन सेवा के रूप में समर्पित स्थिर IP सपोर्ट करता है जिन्हें एक जैसे रिमोट एक्सेस गेटवे चाहिए। [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] Private Internet Access. (n.d.). Strict No-Logs VPN: Stay Secure Online.

https://www.privateinternetaccess.com/vpn-features/no-logs-vpn

[2] Private Internet Access Support. (2026). Understanding Basic Settings on the PIA Client.

https://helpdesk.privateinternetaccess.com/hc/en-us/articles/46777033424923-Understanding-Basic-Settings-on-the-PIA-Client

[3] Private Internet Access Support. (2026). Understanding Advanced Settings on the Desktop PIA Client.

https://helpdesk.privateinternetaccess.com/hc/en-us/articles/46813740976667-Understanding-Advanced-Settings-on-the-Desktop-PIA-Client

[4] Private Internet Access Support. (2026). Understanding the Multi-Hop Feature.

https://helpdesk.privateinternetaccess.com/hc/en-us/articles/46776477273627-Understanding-the-Multi-Hop-Feature

[5] Private Internet Access. (2025). VPN Port Forwarding: The Ultimate Guide.

https://helpdesk.privateinternetaccess.com/hc/en-us/articles/46701354754843-Next-Generation-Port-Forwarding

[6] Private Internet Access. (n.d.). About Us.

https://www.privateinternetaccess.com/about-us

[7] Kape Technologies plc. (2019). Completion of Private Internet Access Acquisition.

https://www.investegate.co.uk/announcement/rns/kape-technologies--kape/completion-of-private-internet-access-acquisition/5834879

[8] Private Internet Access. (n.d.). Private Internet Access - Free and Open Source Software.

https://github.com/pia-foss

[9] Private Internet Access. (n.d.). pia-foss/desktop: Private Internet Access - Desktop VPN Client for Windows/macOS/Linux.

https://github.com/pia-foss/desktop

[10] WireGuard. (n.d.). Protocol & Cryptography.

https://www.wireguard.com/protocol/

उत्तर कुंजी: चेकपॉइंट 1 – बहुविकल्पीय

1 प्रश्न 1 — **सही उत्तर: A**

शिक्षण नोट

Private Internet Access VPN का व्यावसायिक नाम क्या है? → PIA VPN

2 प्रश्न 2 — **सही उत्तर: A**

शिक्षण नोट

Private Internet Access का मुख्यालय किस देश में है, जिससे वह अमेरिकी कानूनों के अधीन है? → संयुक्त राज्य अमेरिका

3 प्रश्न 3 — **सही उत्तर: A**

शिक्षण नोट

PIA अपने डेस्कटॉप क्लाइंट में कौन-सा स्वामित्व वाला विज्ञापन-ब्लॉकिंग टूल शामिल करता है? → PIA MACE

4 प्रश्न 4 — **सही उत्तर: A**

शिक्षण नोट

मानक PIA अकाउंट के तहत एक साथ डिवाइस कनेक्शन की सीमा क्या है? → असीमित

5 प्रश्न 5 — **सही उत्तर: A**

शिक्षण नोट

PIA के ऐप उपयोगकर्ताओं को आधुनिक ओपन-सोर्स प्रोटोकॉल WireGuard या OpenVPN चुनने देते हैं।

उत्तर कुंजी: चेकपॉइंट 2 – सही या गलत

6 **प्रश्न 6** — **सही उत्तर: सही**

शिक्षण नोट

Private Internet Access का मुख्यालय अमेरिका में है और वह Five Eyes क्षेत्राधिकार के अधीन है।

7 **प्रश्न 7** — **सही उत्तर: सही**

शिक्षण नोट

PIA ने अमेरिकी संघीय अदालत के सम्मनों में अपनी ज़ीरो-लॉग नीति साबित की है।

8 **प्रश्न 8** — **सही उत्तर: सही**

शिक्षण नोट

PIA MACE विज्ञापन ब्लॉकिंग DNS अनुरोधों को फ़िल्टर करके क्लाइंट के भीतर काम करती है।

9 **प्रश्न 9** — **सही उत्तर: गलत**

शिक्षण नोट

गलत: PIA चुने हुए सर्वरों पर बिल्ट-इन पोर्ट फ़ॉरवर्डिंग देता है।

10 **प्रश्न 10** — **सही उत्तर: सही**

शिक्षण नोट

सभी PIA डेस्कटॉप क्लाइंट एप्लिकेशन पूरी तरह ओपन-सोर्स हैं।

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

H 1. PIA VPN	F 2. संयुक्त राज्य अमेरिका	B 3. PIA MACE	G 4. असीमित
C 5. WireGuard	E 6. अदालत में प्रमाणित	D 7. Kill Switch	A 8. टनलिंग

चेकपॉइंट 3: उत्तर – प्रमुख शब्द

1 सॉफ़्टवेयर	2 संरक्षण	3 फ़ायरवॉल	4 असीमित
5 वायरगार्ड	6 अदालत प्रमाणित		

चेकपॉइंट 6, वैकल्पिक: उत्तर – शब्द मिलान

1 C – अदालतप्रमाणित	2 F – हार्डवेयर	3 H – संरक्षण	4 G – प्रमाणीकरण
5 B – वायरगार्ड	6 D – फ़ायरवॉल	7 E – सॉफ़्टवेयर	8 A – असीमित

शिक्षकों के लिए चर्चा नोट

प्रमुख शब्द:
जाँचें कि क्या विद्यार्थी PIA VPN, संयुक्त राज्य अमेरिका और PIA MACE 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।

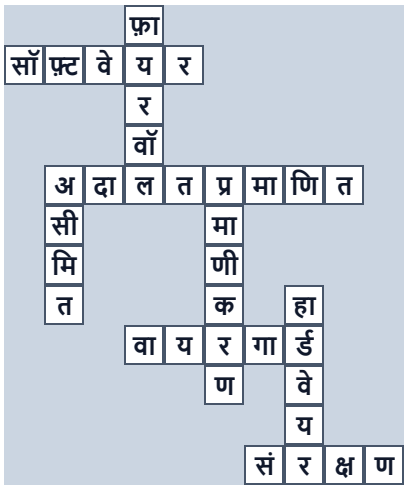
स्रोतों का मूल्यांकन:
विद्यार्थियों से वर्कशीट के स्रोतों में कम से कम एक कथन की पुष्टि करवाएँ और चर्चा करें कि आँकड़े, कीमतें और नियम समय के साथ क्यों बदल सकते हैं।

पहेलियों की कुंजियाँ और शिक्षक नोट

शब्द खोज समाधान

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

क्रॉसवर्ड समाधान



क्रॉसवर्ड समाधान के लिए शिक्षक गाइड

बाएँ से दाएँ

2 बाएँ से दाएँ: सॉफ़्टवेयर कंप्यूटर या फ़ोन पर चलने वाले प्रोग्रामों का समूह (5 अक्षर)

3 बाएँ से दाएँ: अदालतप्रमाणित कानूनी अनुरोधों से सत्यापित लॉग नीति, जिनसे कोई डेटा नहीं मिला (8 अक्षर)

6 बाएँ से दाएँ: वायरगार्ड आधुनिक, उच्च-गति वाला ओपन-सोर्स कनेक्शन प्रोटोकॉल (5 अक्षर)

7 बाएँ से दाएँ: संरक्षण किसी चीज़ को नुकसान और ख़तरे से बचाकर रखना (4 अक्षर)

ऊपर से नीचे

1 ऊपर से नीचे: फ़ायरवॉल अनचाहे नेटवर्क ट्रैफ़िक को रोकने वाली सुरक्षा दीवार (5 अक्षर)

3 ऊपर से नीचे: असीमित बिना सीमा की समवर्ती डिवाइस कनेक्शन नीति (4 अक्षर)

4 ऊपर से नीचे: प्रमाणीकरण पासवर्ड या कोड से साबित करना कि उपयोगकर्ता वही है जो वह कहता है (6 अक्षर)

5 ऊपर से नीचे: हार्डवेयर कंप्यूटर या सर्वर के भौतिक पुर्ज़े और मशीनें (5 अक्षर)

अक्षर-फेर शब्द और कूट संदेश हल कुंजी

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

शब्द अनस्क्रैम्बल कुंजी

1. मि अ त सी — **असीमित**
2. त अ त दा णि मा प्र ल — **अदालतप्रमाणित**
3. वे सॉ र य फ़ट — **सॉफ़्टवेयर**
4. ण क णी र प्र मा — **प्रमाणीकरण**
5. र र्ड वा गा य — **वायरगार्ड**
6. वॉ फ़ा र ल य — **फ़ायरवॉल**
7. य र हा वे र्ड — **हार्डवेयर**
8. सं ण क्ष र — **संरक्षण**

गुप्त कूट चुनौती कुंजी

"पिया वीपीएन सुरक्षा और गोपनीयता देता"

केस स्टडी के उत्तर

A केस स्टडी 1: अदालत में प्रमाणित ज़ीरो लॉग्स का सत्यापन

शिक्षक समाधान

ग्रेडिंग दिशानिर्देश

छात्रों के उत्तरों में निम्नलिखित बिंदु शामिल होने चाहिए:

- परिदृश्य विश्लेषण: एक सरकारी एजेंसी साइबर अपराध जाँच के दौरान किसी विशिष्ट IP पते के कनेक्शन लॉग माँगते हुए PIA को सबपीना जारी करती है।
- अनुशंसित रणनीति और समाधान: मूल्यांकन मार्गदर्शन: समझाएँ कि PIA का सर्वर डेटाबेस डिस्क पर कोई लॉग या मेटाडेटा लिखने के लिए कॉन्फ़िगर नहीं है, इसलिए उनके पास सौंपने के लिए उपयोगकर्ता का कोई इतिहास नहीं है।

B केस स्टडी 2: कस्टम पोर्ट फ़ॉरवर्डिंग कॉन्फ़िगर करना

शिक्षक समाधान

ग्रेडिंग दिशानिर्देश

छात्रों के उत्तरों में निम्नलिखित बिंदु शामिल होने चाहिए:

- परिदृश्य विश्लेषण: एक सॉफ़्टवेयर इंजीनियर एक अस्थायी लोकल सेवा होस्ट करके उसे सुरक्षित VPN पोर्ट आवंटन से रिमोट टेस्टरों के साथ साझा करना चाहता है।
- अनुशंसित रणनीति और समाधान: मूल्यांकन मार्गदर्शन: समझाएँ कि क्लाइंट सर्वर से एक इनकमिंग पोर्ट माँगता है, जो आने वाले ट्रैफ़िक को रीडायरेक्ट करता है; इसका समझौता यह है कि पोर्ट स्कैनिंग की संवेदनशीलता बढ़ जाती है।