نام: _____ تاریخ: _____ نمبر: _____

TunnelBear کا جائزہ

کینیڈا میں قائم TunnelBear کا تکنیکی تجزیہ، VigilantBear kill switch، GhostBear obfuscation، سالانہ آزاد سیکیورٹی آڈٹس، اور زیرو لاگز۔

TunnelBear جائزہ: سیکھنے کا خلاصہ

سیکھنے والا
طالب علم کی حیثیت
نیٹ ورک ڈیفینڈر ٹریک

محفوظ
کنکشن کی صورتحال
ڈیٹا پیکٹس کی حفاظت

فعال
لیک سے تحفظ
DNS اور IPv6 لیک سے تحفظ

خوش آمدید! یہ سرگرمی پیکٹ آپ کو TunnelBear کے تکنیکی جائزے سے متعارف کراتا ہے۔ آپ GhostBear اوبفسکیشن، VigilantBear کِل سوئچ سیٹنگز، اور سالانہ سیکیورٹی آڈٹ کی توثیقات کا جائزہ لیں گے۔

ورک شیٹ کے چیک پوائنٹس

- [ ] **حصہ 1-4: VPN اور نیٹ ورک سیکیورٹی کنفیگریشنز میں مہارت حاصل کریں۔**
- [ ] **حصہ 5-7: کراس ورڈ اور ورڈ سرچ پہیلیاں حل کریں۔**
- [ ] **حصہ 8-9: کیس اسٹڈیز اور سائفر چیلنج حل کریں۔**
- [ ] **حصہ 10: بنیادی اور اعلیٰ FAQ صفحات کا جائزہ لیں۔**
- [ ] **حصہ 11: 10 دلچسپ حقیقی دنیا کے حقائق دریافت کریں۔**
- [ ] **اضافی: تیزی سے سوچیں چیلنج**

VPN.com بہترین VPNs گائیڈ کھولیں

URL: https://www.vpn.com/vpn/tunnelbear/

آپ کا TunnelBear لرننگ روڈ میپ

- TunnelBear جائزے کے تکنیکی فن تعمیر اور خفیہ کاری کے معیارات کا تجزیہ کریں۔
- IP، DNS اور WebRTC ٹریفک لیکس کو روکنے کے لیے کلائنٹ کی سیٹنگز ترتیب دیں۔
- ملکیتی ٹنلنگ پروٹوکولز کا معیاری نفاذ سے موازنہ کریں۔

TunnelBear جائزہ: ہدایات

کثیر انتخابی اور درست/غلط سوالات حل کریں، لفظوں کے ذخیرے کی مدد سے خالی جگہیں پُر کریں، تعریفوں کا ملان کریں، اور کراس ورڈ اور ورڈ سرچ پہیلیاں حل کریں۔ اپنے علم کو GhostBear اوبفسکیشن اور VigilantBear سوئچز پر لاگو کریں۔ اور آخر میں اضافی سرگرمی "تیزی سے سوچیں"۔

GhostBear آبفسکیشن اور سالانہ آزاد آڈٹ کی تصدیق

TunnelBear اپنے سالانہ آزاد سیکیورٹی آڈٹس کے لیے مشہور ہے جو Cure53 کرتی ہے۔ اس کا صدر دفتر کینیڈا میں ہے، اور یہ DPI سنسرز کو بائی پاس کرنے کے لیے GhostBear پروٹوکول اوبفسکیشن، VigilantBear کنکشن لیک تحفظ، اور لامحدود ڈیوائس لنکس پیش کرتا ہے۔

(تعارف)

TunnelBear اپنے سالانہ آزاد سیکیورٹی آڈٹس کے لیے مشہور ہے جو Cure53 کرتی ہے۔ اس کا صدر دفتر کینیڈا میں ہے، اور یہ DPI سنسرز کو بائی پاس کرنے کے لیے GhostBear پروٹوکول اوبفسکیشن، VigilantBear کنکشن لیک تحفظ، اور لامحدود ڈیوائس لنکس پیش کرتا ہے۔

ہر چیک پوائنٹ کو غور سے پڑھیں اور درست جواب منتخب کریں یا لکھیں۔

چیک پوائنٹ 1: کثیر انتخابی چیلنج

1. TunnelBear کا کارپوریٹ ادارہ کس ملک میں رجسٹرڈ ہے؟
   - A) کینیڈا
   - B) ریاستہائے متحدہ
   - C) سوئٹزرلینڈ
   - D) جرمنی

2. TunnelBear کی سنسرشپ کو بائی پاس کرنے والی ابفسکیشن کا نام کیا ہے؟
   - A) GhostBear
   - B) Chameleon
   - C) Stealth
   - D) ShadowSocks

3. TunnelBear کی بلٹ اِن کِل سوئچ خصوصیت کا نام کیا ہے؟
   - A) VigilantBear
   - B) Secure Core
   - C) NetShield
   - D) SafePath

4. کس سائبر سیکیورٹی فرم نے 2018 میں TunnelBear کو حاصل کیا؟
   - A) McAfee
   - B) Avast
   - C) NortonLifeLock
   - D) Kape Technologies

5. TunnelBear جدید تیز رفتار ٹنلز کے لیے کون سا پروٹوکول تجویز کرتا ہے؟
   - A) WireGuard
   - B) OpenVPN
   - C) IKEv2
   - D) PPTP

چیک پوائنٹ 2: درست یا غلط چیلنج

6 سوال 6

6. GhostBear، ڈیپ پیکٹ انسپیکشن فائر والز کو بائی پاس کرنے میں مدد کے لیے VPN میٹا ڈیٹا کو گڈمڈ کرتا ہے۔

درست ○ غلط ○

7 سوال 7

7. TunnelBear کے مفت پلان میں ماہانہ لامحدود براؤزنگ ڈیٹا شامل ہے۔

درست ○ غلط ○

8 سوال 8

8. VigilantBear ایپ کے کنکٹ یا دوبارہ کنکٹ ہوتے وقت ڈیٹا کو محفوظ رکھتا ہے۔

درست ○ غلط ○

9 سوال 9

9. TunnelBear پہلا صارفی VPN تھا جس نے سالانہ عوامی سیکیورٹی آڈٹس شائع کیے۔

درست ○ غلط ○

10 سوال 10

10. فراہم کنندہ پانامہ کے قوانین کے سخت دائرہ اختیار کے تحت کام کرتا ہے۔

درست ○ غلط ○

چیک پوائنٹ 3: کلیدی اصطلاح شامل کرنا

ذیل میں ہر جملہ پڑھیں اور خالی جگہ کو ورڈ بینک سے درست اصطلاح کے ساتھ پُر کریں۔

1. TunnelBear کا صدر دفتر اور آپریشنز سخت قوانین والے ملک _____ میں ہیں۔
2. اوبفسکیشن ٹیکنالوجی _____ سسٹم سیٹنگز سے چلتی ہے۔
3. سسٹم سطح کا لیک تحفظ _____ سیٹنگز سے منظم ہوتا ہے۔
4. وی پی این فراہم کنندہ کو 2018 میں سیکیورٹی ڈیولپر _____ نے خرید لیا۔
5. تیز ڈیٹا ترسیلی رفتار _____ پروٹوکول کے ذریعے حاصل ہوتی ہے۔
6. روایتی ڈیسک ٹاپ کلائنٹ کنکشنز _____ پروٹوکول پر انحصار کرتے ہیں۔

الفاظ کا بینک

آڈٹ | کینیڈا | گھوسٹ بیئر | میکیفی | نو لاگز | وائر گارڈ | وجیلنٹ بیئر | OpenVPN

اپنے جوابات یہاں لکھیں:

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

چیک پوائنٹ 4: VPN اور نیٹ ورک تصورات کا ملان

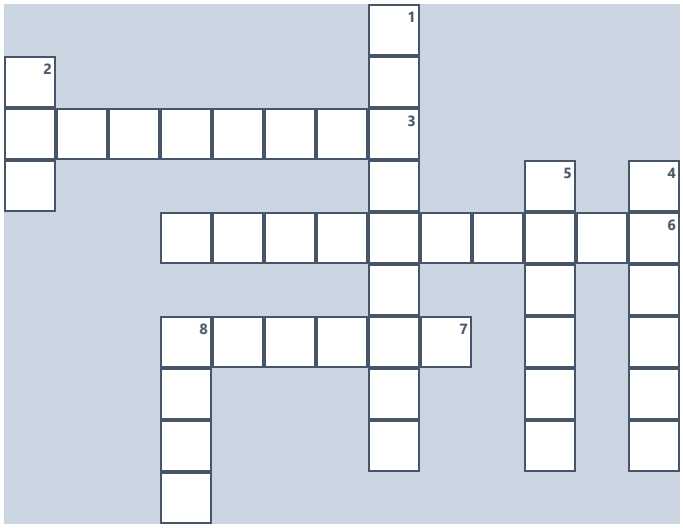
تعریفوں کا ملان

دائیں جانب کی ہر اصطلاح کو بائیں جانب کی درست تعریف سے ملائیں اور بھرے جانے والے ان پٹ باکس میں متعلقہ حرف (A-H) لکھیں۔

1. کینیڈا	A	پرائیویسی پالیسی جو ٹریفک ہسٹری برقرار نہ رکھنے کو نافذ کرتی ہے۔
2. GhostBear	B	رجسٹریشن کا ملک اور کارپوریٹ صدر دفتر۔
3. VigilantBear	C	تھرڈ پارٹی سیکیورٹی جائزہ جو سالانہ کیا جاتا ہے۔
4. McAfee	D	ڈیسک ٹاپس پر استعمال ہونے والا معیاری اوپن سورس ٹنلنگ پروٹوکول۔
5. WireGuard	E	سیکیورٹی پیرنٹ کارپوریشن جس نے TunnelBear کو حاصل کیا۔
6. OpenVPN	F	جدید کرپٹوگرافی استعمال کرنے والا اعلیٰ کارکردگی کا پروٹوکول۔
7. آڈٹ	G	میٹا ڈیٹا کی بدل پھیر کی ٹیکنالوجی جو ڈیپ پیکٹ انسپیکشن سے بچنے کے لیے استعمال ہوتی ہے۔
8. زیرو لاگز	H	بلٹ اِن کِل سوئچ جو کنکشن ٹوٹنے کے دوران کنکشنز کی حفاظت کرتا ہے۔

چیک پوائنٹ 5: کراس ورڈ پہیلی

فعال سفید خانوں میں حروف ٹائپ کر کے کراس ورڈ پہیلی حل کریں۔ نمبر نیچے دیے گئے سراغوں سے مطابقت رکھتے ہیں۔



افقی

3. جدید کرپٹوگرافی استعمال کرنے والا اعلیٰ کارکردگی کا پروٹوکول (8)

6. ڈراپ ہونے کی صورت میں کنکشن کو تحفظ دینے والا بلٹ اِن کل سوئچ (10)

7. رجسٹریشن کا ملک اور کارپوریٹ صدر دفتر (6)

عمودی

1. میٹا ڈیٹا کو گڈمڈ کرنے کی ٹیکنالوجی جو ڈیپ پیکٹ انسپیکشن کو بائی پاس کرتی ہے (9)

2. تیسرے فریق کی سیکیورٹی جانچ جو ہر سال کی جاتی ہے (3)

4. رازداری کی پالیسی جو ٹریفک ہسٹری محفوظ نہ رکھنے کو نافذ کرتی ہے (6)

5. سیکیورٹی کی وہ مادر کمپنی جس نے TunnelBear کو خریدا (6)

8. ڈیسک ٹاپس پر استعمال ہونے والا معیاری کھلے کوڈ کا ٹنلنگ پروٹوکول (4)

چیک پوائنٹ 5 – متبادل سرگرمی: قابلِ رسائی کراس ورڈ سراغ

اسکرین ریڈر اور کی بورڈ استعمال کرنے والے صارفین نیچے دیے گئے ٹیکسٹ فیلڈز میں کراس ورڈ کے جوابات براہ راست ٹائپ کر سکتے ہیں۔

افقی

3 افقی: جدید کرپٹوگرافی استعمال کرنے والا اعلیٰ کارکردگی کا پروٹوکول (8 حروف):

6 افقی: ڈراپ ہونے کی صورت میں کنکشن کو تحفظ دینے والا بلٹ اِن کل سوئچ (10 حروف):

7 افقی: رجسٹریشن کا ملک اور کارپوریٹ صدر دفتر (6 حروف):

عمودی

1 عمودی: میٹا ڈیٹا کو گڈمڈ کرنے کی ٹیکنالوجی جو ڈیپ پیکٹ انسپیکشن کو بائی پاس کرتی ہے (9 حروف):

2 عمودی: تیسرے فریق کی سیکیورٹی جانچ جو ہر سال کی جاتی ہے (3 حروف):

4 عمودی: رازداری کی پالیسی جو ٹریفک ہسٹری محفوظ نہ رکھنے کو نافذ کرتی ہے (6 حروف):

5 عمودی: سیکیورٹی کی وہ مادر کمپنی جس نے TunnelBear کو خریدا (6 حروف):

8 عمودی: ڈیسک ٹاپس پر استعمال ہونے والا معیاری کھلے کوڈ کا ٹنلنگ پروٹوکول (4 حروف):

چیک پوائنٹ 6: پوشیدہ الفاظ کی تلاش

نیچے گرڈ میں چھپی 8 اہم اصطلاحات تلاش کریں۔ الفاظ افقی، عمودی یا ترچھے ہو سکتے ہیں۔

ف	ت	ل	س	ف	ک	چ	ج	ل	ز	ش	ش	ھ	ہ	ت
ئ	ا	ر	پ	ک	س	ٹ	ب	ن	ن	ز	ر	ر	ک	م
ب	د	پ	ٹ	ل	ہ	ز	ج	چ	ب	گ	ر	ٹ	ھ	ی
ن	ٹ	ی	ٹ	ہ	ٹ	ک	ا	ش	د	ا	ل	ئ	س	ف
چ	ل	ج	ا	ا	ز	ف	ج	ڈ	ئ	ل	ئ	م	م	ب
ب	ب	ل	ش	ڈ	و	ت	ب	د	ی	و	ہ	ے	ٹ	و
ٹ	ل	ک	ڈ	ر	و	پ	ز	ی	ٹ	ن	م	ڈ	ک	چ
چ	ے	ر	ش	ڈ	د	ئ	ن	چ	ف	ئ	ی	ہ	د	ی
ڈ	ر	ا	گ	ر	ئ	ا	و	ب	ز	ہ	ک	ک	م	ل
ھ	ڈ	ی	ر	ت	گ	ھ	و	س	ٹ	ب	ی	ئ	ر	ن
ت	ت	و	م	ی	ج	ف	م	چ	ٹ	ک	ف	س	ج	ٹ
ڈ	د	ر	ہ	ن	ہ	ا	ے	ز	ز	ے	ی	س	گ	ب
ا	ب	ک	ی	ز	ی	گ	ا	چ	ش	ز	پ	ے	ے	ی
د	ب	و	ر	ک	ش	ی	ب	ی	ئ	ش	ش	ز	ئ	ئ
ر	ک	ٹ	ڈ	ا	ٹ	ی	ب	ٹ	ا	ے	ہ	و	ٹ	ر

الفاظ کی فہرست

کینیڈا
گھوسٹبیئر
وجیلنٹبیئر
میکیفی
وائرگارڈ
اوپن
اڈٹ
نولاگز

چیک پوائنٹ 6 – متبادل سرگرمی: قابلِ رسائی الفاظ کا ملان

ورڈ سرچ کی 8 اصطلاحات میں سے ہر ایک کو اس کی درست تعریف سے ملائیں اور خالی جگہ میں حرف (A-H) لکھیں۔

اصطلاحات
A. کینیڈا
B. گھوسٹبیئر
C. وجیلنٹبیئر
D. میکیفی
E. وائرگارڈ
F. اوپن
G. اڈٹ
H. نولاگز

تعریفیں اور ملان کے خانے
1. ڈیسک ٹاپس پر استعمال ہونے والا معیاری کھلے کوڈ کا ٹنلنگ پروٹوکول۔
2. رازداری کی پالیسی جو ٹریفک ہسٹری محفوظ نہ رکھنے کو نافذ کرتی ہے۔
3. جدید کرپٹوگرافی استعمال کرنے والا اعلیٰ کارکردگی کا پروٹوکول۔
4. رجسٹریشن کا ملک اور کارپوریٹ صدر دفتر۔
5. تیسرے فریق کی سیکیورٹی جانچ جو ہر سال کی جاتی ہے۔
6. میٹا ڈیٹا کو گڈمڈ کرنے کی ٹیکنالوجی جو ڈیپ پیکٹ انسپیکشن کو بائی پاس کرتی ہے۔
7. سیکیورٹی کی وہ مادر کمپنی جس نے TunnelBear کو خریدا۔
8. ڈراپ ہونے کی صورت میں کنکشن کو تحفظ دینے والا بلٹ اِن کل سوئچ۔

چیک پوائنٹ 7: الجھے الفاظ کا چیلنج

ورچوئل پرائیویٹ نیٹ ورک (VPN) کے اہم تصورات اور اصطلاحات ظاہر کرنے کے لیے نیچے دیے گئے حروف کو درست ترتیب میں لائیں۔ اپنے جوابات دیے گئے ان پٹ باکسز میں لکھیں۔

1. ن ک ی ڈ ا ی
2. ئ ل و ج ن ر ب ی ٹ ی
3. ر ا و گ ا ڈ ر ئ
4. ڈ ٹ ا
5. ی ٹ ھ ر ب س گ ئ و
6. ف ی م ک ی ی
7. پ ا ن و
8. ل ز ن گ ا و

اضافی سرگرمی: تیزی سے سوچیں

ہر زمرے کے لیے 3 جوابات لکھیں۔ جو سب سے پہلے فہرست مکمل کرے وہ جیتتا ہے۔

1	وہ ممالک جہاں آپ TunnelBear کے سرورز چاہیں گے		
2	وہ چیزیں جو TunnelBear آپ کے نیٹ ورک سے چھپا سکتا ہے		
3	وہ حالات جن میں کل سوئچ مددگار ہوتا ہے		
4	اس ورک شیٹ میں سیکھے گئے سیکیورٹی کے الفاظ		
5	آپ کے جانے پہچانے VPN پروٹوکولز کے نام		
6	وہ ڈیوائسز جن پر آپ TunnelBear انسٹال کریں گے		
7	وہ مقامات جہاں آپ TunnelBear آن کریں گے		
8	وہ ایپس جو آپ TunnelBear کے ساتھ استعمال کریں گے		
9	VPN کنکشن کے سست ہونے کی علامات		
10	VPN خریدنے سے پہلے جانچنے کی چیزیں		
11	اچھی VPN ایپ کو بیان کرنے والے الفاظ		
12	VPN ایپ میں موجود بٹنوں یا مینیو کے نام		
13	وہ اسٹریمنگ سروسز جو آپ دیکھتے ہیں		
14	وہ ڈیٹا جو VPN کو کبھی محفوظ نہیں کرنا چاہیے		
15	TunnelBear میں وہ خصوصیات جن کی آپ تلاش کرتے ہیں		

چیک پوائنٹ 8: VPN اور نیٹ ورک کیس اسٹڈیز

جو تصورات آپ نے سیکھے ہیں انہیں نیچے دیے گئے حقیقی منظرناموں کو حل کرنے میں استعمال کریں۔

کیس اسٹڈی 1: سنسرشپ سے بچاؤ



منظرنامہ: ایک محقق ایسے ملک سے گزر رہا ہے جو VPN پروٹوکولز کو بلاک کرتا ہے، اور اسے تحقیقی مواد تک رسائی چاہیے۔

بحث کا سوال: ڈیپ پیکٹ انسپیکشن کو بائی پاس کرنے کے لیے TunnelBear کی کون سی سیٹنگ فعال کی جانی چاہیے؟

کیس اسٹڈی 2: غیر محفوظ عوامی ہاٹ اسپاٹس



منظرنامہ: ایک انجینئر ایئرپورٹ کے کھلے Wi-Fi ہاٹ اسپاٹ سے کنیکٹ ہوتا ہے اور بار بار کنکشن ڈراپ ہونے کا سامنا کرتا ہے۔

بحث کا سوال: کنکشن ڈراپ ہونے کے دوران VigilantBear انجینئر کی ڈیوائس کی حفاظت کیسے کرتا ہے؟

چیک پوائنٹ 9: سائفر حل کریں

نیٹ ورک انجینئر روٹنگ چینلز اور کلائنٹ ٹنلز کو محفوظ بناتا ہے۔ نیچے دی گئی حرف سے عدد کی کلید استعمال کر کے خالی جگہوں میں متعلقہ حروف لکھ کر پیغام ڈی کرپٹ کریں۔

حرف سے عدد خفیہ کاری کی کلید

ا=1 ب=2 پ=3 ت=4 ٹ=5 ث=6 ج=7 چ=8 ح=9 خ=10 د=11 ڈ=12 ذ=13

ر=14 ڑ=15 ز=16 ژ=17 س=18 ش=19 ص=20 ض=21 ط=22 ظ=23 ع=24 غ=25 ف=26

ق=27 ک=28 گ=29 ل=30 م=31 ن=32 ں=33 و=34 ہ=35 ھ=36 ی=37 ے=38 ئ=39

38	18	28	37	30	14	39	37	2	5	32	30	37	7	34

1	4	37	11	23	26	9	4

ڈی کوڈ شدہ پیغام:

ٹپ: ہر نمبر اوپر دی گئی کلید کے ایک اردو حرف کو ظاہر کرتا ہے۔

چیک پوائنٹ 10: VPN عمومی سوالات – بنیادی (حصہ A)

ورچوئل پرائیویٹ نیٹ ورکس (VPNs) اور ٹنلنگ کے بارے میں سب سے عام سوالات اور جوابات کا جائزہ لیں۔

Q1: کیا TunnelBear محفوظ ہے؟

ہاں، یہ AES-256 خفیہ کاری استعمال کرتا ہے اور اس کی ایپس کا ہر سال آزادانہ آڈٹ ہوتا ہے۔ [1]

Q2: GhostBear کیا ہے؟

GhostBear ایک آبفسکیشن خصوصیت ہے جو سنسرشپ بلاکس کو بائی پاس کرنے کے لیے VPN ٹریفک کو چھپاتی ہے۔

Q3: کیا اس کا کوئی مفت درجہ ہے؟

جی ہاں، TunnelBear 2GB ماہانہ بینڈوڈتھ ڈیٹا کے ساتھ محدود مفت درجہ پیش کرتا ہے۔ [1]

Q4: TunnelBear کہاں قائم ہے؟

TunnelBear کا صدر دفتر ٹورنٹو، کینیڈا میں ہے، کینیڈا کے دائرہ اختیار کے تحت۔

Q5: VigilantBear کیا ہے؟

VigilantBear، TunnelBear کا بلٹ اِن Kill Switch ہے جو کنکشن ٹوٹنے کے دوران لیکس کو روکتا ہے۔

چیک پوائنٹ 10: VPN عمومی سوالات – بنیادی (حصہ B)

ورچوئل پرائیویٹ نیٹ ورکس (VPNs) اور ٹنلنگ کے بارے میں سب سے عام سوالات اور جوابات کا جائزہ لیں۔

Q6: کیا میں متعدد آلات جوڑ سکتا ہوں؟

ہاں، ادا شدہ پلانز ایک اکاؤنٹ کے تحت لامحدود بیک وقت کنکشنز کو سپورٹ کرتے ہیں۔

Q7: کیا TunnelBear WireGuard کو سپورٹ کرتا ہے؟

جی ہاں، اعلیٰ کارکردگی اور بیٹری کے لحاظ سے مؤثر کنکشنز کے لیے WireGuard سپورٹ کیا جاتا ہے۔

Q8: ان کی زیرو لاگز پالیسی کیا ہے؟

TunnelBear IP ایڈریسز، DNS کوئریز یا صارف کی براؤزنگ سرگرمی لاگ نہیں کرتا۔

Q9: TunnelBear کا مالک کون ہے؟

TunnelBear کو بڑی سائبر سیکیورٹی فرم McAfee نے 2018 میں حاصل کیا۔ [8]

Q10: کیا یہ اشتہارات کو بلاک کرتا ہے؟

TunnelBear خفیہ کاری پر توجہ دیتا ہے؛ ایڈ بلاکنگ بنیادی VPN کلائنٹ میں شامل نہیں ہے۔ [4]

چیک پوائنٹ 10: VPN عمومی سوالات – اعلیٰ (حصہ C)

VPN ٹنلنگ پروٹوکولز، موبائل کلائنٹ انضمام اور انٹرپرائز تعیناتی کے جدید تکنیکی پہلوؤں کا جائزہ لیں۔

Q1: GhostBear DPI سے کیسے بچتا ہے؟

یہ خفیہ VPN ٹریفک کو عام HTTPS جیسا ظاہر کرتا ہے، اس لیے DPI فلٹرز کو اسے پہچاننے میں دشواری ہوتی ہے۔

Q2: کیا کینیڈا Eyes-5 ملک ہے؟

جی ہاں، کینیڈا Five-Eyes اتحاد کا رکن ہے، جس سے دائرۂ اختیار کے حوالے سے غور طلب امور پیدا ہوتے ہیں۔

Q3: VigilantBear ڈیٹا لیکس کو کیسے بلاک کرتا ہے؟

یہ VPN کنکشن دوبارہ قائم ہونے تک تمام آنے اور جانے والے ٹریفک کو بلاک کر دیتا ہے۔

Q4: ان کے آڈٹس میں کن چیزوں کی جانچ کی جاتی ہے؟

Cure53 ایپ کوڈ، سرور کنفیگریشنز، انفراسٹرکچر اور لاگنگ کنٹرولز کا آڈٹ کرتا ہے۔

Q5: کیا WireGuard مقامی طور پر چلتا ہے؟

جی ہاں، TunnelBear ایپس تیز اور مستحکم کنکشنز کے لیے WireGuard پیش کرتی ہیں۔

چیک پوائنٹ 10: VPN عمومی سوالات – اعلیٰ (حصہ D)

VPN ٹنلنگ پروٹوکولز، موبائل کلائنٹ انضمام اور انٹرپرائز تعیناتی کے جدید تکنیکی پہلوؤں کا جائزہ لیں۔

Q6: کیا مخصوص P2P سرورز موجود ہیں؟

نہیں، P2P ٹریفک تمام عالمی سرور نوڈز پر بغیر پابندی کے سپورٹ کیا جاتا ہے۔

Q7: کیا یہ WebRTC لیکس کو روکتا ہے؟

ہاں، کلائنٹ مقامی IP کے انکشاف کو روکنے کے لیے WebRTC درخواستوں کو روک کر روٹ کرتا ہے۔

Q8: DNS سیکیورٹی کا انتظام کیسے کیا جاتا ہے؟

DNS کوئریز TunnelBear کے نجی، خفیہ کردہ DNS ریزولورز کے ذریعے بھیجی جاتی ہیں۔

Q9: کیا میں اسے Linux پر استعمال کر سکتا ہوں؟

TunnelBear کی کوئی سرکاری Linux ایپ نہیں ہے؛ اس کی ایپس Windows، macOS، iOS اور Android کا احاطہ کرتی ہیں۔ [5]

Q10: بلنگ ڈیٹا بیسز کو کیسے الگ رکھا جاتا ہے؟

گمنامی برقرار رکھنے کے لیے بلنگ ریکارڈز سرور ٹریفک لاگز سے الگ محفوظ کیے جاتے ہیں۔

حصہ 11: 10 حقیقی دنیا کے VPN حقائق اور بصیرتیں

VPN خفیہ کاری کی رفتار، پروٹوکول آڈٹس، موبائل کنیکٹیویٹی اور انٹرپرائز ریموٹ ورک کے بارے میں حقیقی دنیا کے حقائق کا جائزہ لیں۔

1. VPN بصیرت

TunnelBear کا صدر دفتر ٹورنٹو، کینیڈا میں ہے اور یہ کینیڈا کے دائرہ اختیار کے تحت کام کرتا ہے۔ [2]

2. VPN بصیرت

سروس کو McAfee نے 2018 میں اپنے سیکیورٹی پورٹ فولیو کو مضبوط بنانے کے لیے حاصل کیا۔ [3]

3. VPN بصیرت

GhostBear، VPN پروٹوکول کے دستخطوں کو اس طرح چھپاتا ہے کہ وہ معیاری HTTP/S پیکٹس جیسے نظر آئیں۔ [4]

4. VPN بصیرت

VigilantBear کلائنٹ کے فائر وال لیول کنکشن Kill Switch کے طور پر کام کرتا ہے۔ [4]

5. VPN بصیرت

ایپ اور سرور کی سیکیورٹی کی تصدیق کے لیے Cure53 سالانہ عوامی آڈٹ کرتی ہے۔ [6]

6. VPN بصیرت

ادا شدہ سبسکرپشنز لامحدود بیک وقت ڈیوائس کنکشنز کو سپورٹ کرتی ہیں۔ [1]

7. VPN کی بصیرت

نیٹ ورک AES-256 خفیہ کاری پر انحصار کرتا ہے، جو عالمی سیکیورٹی معیار ہے۔ [1]

8. VPN کی بصیرت

یہ OpenVPN، IKEv2 اور WireGuard پروٹوکول ٹنلز کو سپورٹ کرتا ہے۔ [5]

9. VPN کی بصیرت

صارف کی منزل کے IP ایڈریسز یا براؤزنگ ہسٹری کے کوئی لاگز نہیں رکھے جاتے۔

10. VPN بصیرت

وہ VPN کے انتظام کو آسان بنانے کے لیے ریچھ کی تھیم والا دلچسپ صارف انٹرفیس پیش کرتے ہیں۔

تکنیکی حوالہ جات اور ماخذ

مطالعاتی گائیڈ اور انٹرایکٹو پہیلیاں عالمی تکنیکی معیارات، تصریحات اور ریگولیٹری فریم ورکس سے مرتب کی گئی ہیں۔

علمی اور صنعتی حوالہ جات

[1] TunnelBear, LLC. (2026). TunnelBear VPN - Apps on Google Play.
https://play.google.com/store/apps/details?id=com.tunnelbear.android&hl=en_US

[2] TunnelBear, LLC. (n.d.). TunnelBear: Safe and Fast VPN App - App Store.
https://apps.apple.com/us/app/tunnelbear-secure-vpn-wifi/id564842283

[3] TechCrunch. (2018). McAfee acquires VPN company TunnelBear.
https://techcrunch.com/2018/03/08/mcafee-acquires-vpn-company-tunnelbear/

[4] PCWorld. (2024). TunnelBear VPN review: It's just right for beginners.
https://www.pcworld.com/article/406999/tunnelbear-vpn-review-2.html

[5] CyberInsider. (2026). TunnelBear Review & Test Results 2026 — Pros and Cons.
https://cyberinsider.com/vpn/reviews/tunnelbear/

[6] Cure53. (2024). Pentest-Report TunnelBear VPN Clients & Servers 10-11.2023.
https://cure53.de/pentest-report_tunnelbear_2023.pdf

[7] Cure53. (2020). TunnelBear Security Assessment Summary 11.2019.
https://cure53.de/summary-report_tunnelbear_2019.pdf

[8] VentureBeat. (2018). McAfee acquires VPN provider TunnelBear.
https://venturebeat.com/2018/03/08/mcafee-acquires-vpn-company-tunnelbear/

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

[10] Office of the Privacy Commissioner of Canada. (n.d.). The Personal Information Protection and Electronic Documents Act (PIPEDA).
https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/

جوابی کلید: چیک پوائنٹ 1 – کثیر انتخابی

1 سوال 1 — درست جواب: **A**

تدریسی نوٹ

TunnelBear کا کارپوریٹ ادارہ کس ملک میں رجسٹرڈ ہے؟ → کینیڈا

2 سوال 2 — درست جواب: **A**

تدریسی نوٹ

TunnelBear کی سنسرشپ کو بائی پاس کرنے والی ابفسکیشن کا نام کیا ہے؟ → GhostBear

3 سوال 3 — درست جواب: **A**

تدریسی نوٹ

TunnelBear کی بلٹ اِن کِل سوئچ خصوصیت کا نام کیا ہے؟ → VigilantBear

4 سوال 4 — درست جواب: **A**

تدریسی نوٹ

کس سائبر سیکیورٹی فرم نے 2018 میں TunnelBear کو حاصل کیا؟ → McAfee

5 سوال 5 — درست جواب: **A**

تدریسی نوٹ

TunnelBear جدید تیز رفتار ٹنلز کے لیے کون سا پروٹوکول تجویز کرتا ہے؟ → WireGuard

جوابی کلید: چیک پوائنٹ 2 – درست یا غلط

6 سوال 6

درست جواب: درست

تدریسی نوٹ

درست: GhostBear VPN ٹریفک کو چھپاتا ہے تاکہ وہ ڈیپ پیکٹ انسپیکشن سے گزر سکے۔

7 سوال 7

درست جواب: غلط

تدریسی نوٹ

غلط: فری پلان ہر ماہ 2GB براؤزنگ ڈیٹا دیتا ہے۔

8 سوال 8

درست جواب: درست

تدریسی نوٹ

VigilantBear ایپ کے کنکٹ یا دوبارہ کنکٹ ہوتے وقت ڈیٹا کو محفوظ رکھتا ہے۔

9 سوال 9

درست جواب: درست

تدریسی نوٹ

درست: TunnelBear کا کہنا ہے کہ وہ سالانہ عوامی تھرڈ پارٹی آڈٹس مکمل کرنے والا پہلا کنزیومر VPN تھا۔

10 سوال 10

درست جواب: غلط

تدریسی نوٹ

غلط: TunnelBear ٹورنٹو میں قائم ہے اور کینیڈین قانون کے تحت کام کرتا ہے۔

الفاظ کی کلید اور درجہ بندی کا معیار

استاد کی گریڈنگ روبرک: ہر درست ملان (کل 8 نمبر) اور سیاقی اصطلاح (کل 6 نمبر) کے لیے 1 نمبر دیں۔

چیک پوائنٹ 4: جوابی کلید – تصورات کا ملان

B 1. کینیڈا	G 2. GhostBear	H 3. VigilantBear	E 4. McAfee
F 5. WireGuard	D 6. OpenVPN	C 7. آڈٹ	A 8. زیرو لاگز

چیک پوائنٹ 3: جوابی کلید – اہم اصطلاحات

1 کینیڈا	2 گھوسٹ بیئر	3 وجیلنٹ بیئر	4 میکیفی
5 وائر گارڈ	6 OpenVPN		

چیک پوائنٹ 6 – متبادل سرگرمی: جوابی کلید – الفاظ کا ملان

1 F – اوپن	2 H – نولاگز	3 E – وائرگارڈ	4 A – کینیڈا
5 G – اڈٹ	6 B – گھوسٹبیئر	7 D – میکیفی	8 C – وجیلنٹبیئر

اساتذہ کے لیے بحث کے نوٹس

اہم اصطلاحات:
یقینی بنائیں کہ طلبہ کینیڈا، GhostBear اور VigilantBear کو اپنے الفاظ میں سمجھا سکیں اور ہر ایک کی مثال دے سکیں۔

کیس اسٹڈیز:
طلبہ سے کہیں کہ اپنی سفارشات کو ورک شیٹ کے حقائق پر مبنی رکھیں، ذاتی رائے پر نہیں۔

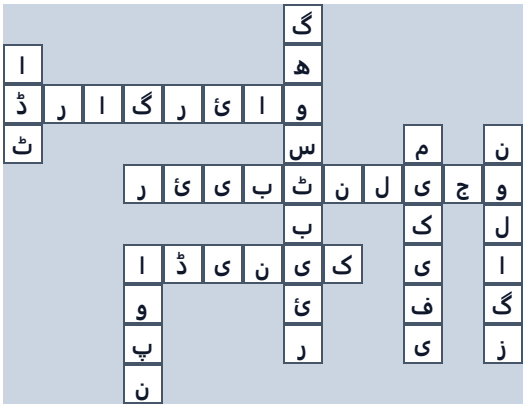
ماخذ کی جانچ:
طلبہ سے کہیں کہ ورک شیٹ کے ماخذ میں کم از کم ایک دعوے کی تصدیق کریں، اور اس پر بات کریں کہ اعداد و شمار، قیمتیں اور قواعد وقت کے ساتھ کیوں بدل سکتے ہیں۔

پہیلیوں کی کلیدیں اور استاد کے نوٹس

الفاظ کی تلاش کا حل

ف	ت	ل	س	ف	ک	ج	ج	ل	ز	ش	ش	ھ	ہ	ت
ئ	ا	ر	پ	ک	س	ٹ	ب	ن	ن	ز	ر	ر	ک	م
ب	د	پ	ٹ	ل	ہ	ز	چ	چ	ب	گ	ر	ٹ	ھ	ی
ن	ٹ	ی	ٹ	ہ	ٹ	ک	ا	ش	د	ا	ل	ئ	س	ف
چ	ل	چ	ا	ا	ز	ف	چ	ڈ	ئ	ل	ئ	م	م	ب
ب	ب	ل	ش	ڈ	و	ت	ب	د	ی	و	ہ	ے	ٹ	و
ٹ	ل	ک	ڈ	ر	و	پ	ز	ی	ٹ	ن	م	ڈ	ک	چ
چ	ے	ر	ش	ڈ	د	ئ	ن	چ	ف	ئ	ی	ہ	د	ی
ڈ	ر	ا	گ	ر	ئ	ا	و	ب	ز	ہ	ک	ک	م	ل
ھ	ڈ	ی	ٹ	ر	ت	گ	ھ	س	ٹ	ب	ی	ئ	ر	ن
ت	ت	و	م	ی	چ	ف	م	چ	ٹ	ک	ف	س	چ	ٹ
ت	د	ر	ہ	ن	ہ	ا	ے	ز	ز	ے	ی	س	گ	ب
ا	ب	ک	ی	ز	ی	گ	ا	چ	ش	ز	پ	ے	ے	ی
د	ب	و	ر	ک	ش	ی	ب	ی	ئ	ش	ش	ز	ئ	ئ
ر	ک	ٹ	ڈ	ا	ٹ	ی	ب	ٹ	ا	ے	ہ	و	ٹ	ر

کراس ورڈ کا حل



کراس ورڈ حل کے لیے استاد کی گائیڈ

افقی

3 افقی: وائرگارڈ جدید کرپٹوگرافی استعمال کرنے والا اعلیٰ کارکردگی کا پروٹوکول (8 حروف)

6 افقی: وجیلنٹبیئر ڈراپ ہونے کی صورت میں کنکشن کو تحفظ دینے والا بلٹ اِن کل سوئچ (10 حروف)

7 افقی: کینیڈا رجسٹریشن کا ملک اور کارپوریٹ صدر دفتر (6 حروف)

عمودی

1 عمودی: گھوسٹبیئر میٹا ڈیٹا کو گڈمڈ کرنے کی ٹیکنالوجی جو ڈیپ پیکٹ انسپیکشن کو بائی پاس کرتی ہے (9 حروف)

2 عمودی: اڈٹ تیسرے فریق کی سیکیورٹی جانچ جو ہر سال کی جاتی ہے (3 حروف)

4 عمودی: نولاگز رازداری کی پالیسی جو ٹریفک ہسٹری محفوظ نہ رکھنے کو نافذ کرتی ہے (6 حروف)

5 عمودی: میکیفی سیکیورٹی کی وہ مادر کمپنی جس نے TunnelBear کو خریدا (6 حروف)

8 عمودی: اوپن ڈیسک ٹاپس پر استعمال ہونے والا معیاری کھلے کوڈ کا ٹنلنگ پروٹوکول (4 حروف)

الفاظ کی ترتیب اور سائفر حل کی کلید

الفاظ کی ترتیب درست کرنے کی سرگرمی اور Secret Cipher Challenge کی گریڈنگ کلید۔

الفاظ کی ترتیب درست کرنے کی کلید

1. نکیڈای — کینیڈا
2. ئلوجنربیٹی — وجیلنٹبیئر
3. راوگاڈرئ — وائرگارڈ
4. ڈٹا — اڈٹ
5. یٹھربسگئو — گھوسٹبیئر
6. فیمکیی — میکیفی
7. پانو — اوپن
8. لزنگاو — نولاگز

خفیہ سائفر چیلنج کی کلید

"وجیلنٹ بیئر لیک سے تحفظ دیتا"

کیس اسٹڈیز کی جوابی کلید

A کیس اسٹڈی 1: سنسرشپ سے بچاؤ

استاد کا حل

گریڈنگ کی ہدایت

طلبہ کے جوابات میں درج ذیل نکات شامل ہونے چاہییں:

- منظرنامے کا تجزیہ: ایسے ملک سے گزرنے والے محقق کو، جو VPN پروٹوکولز بلاک کرتا ہے، تحقیقی مواد تک رسائی چاہیے۔
- تجویز کردہ حکمت عملی اور حل: VPN پیکٹ میٹا ڈیٹا کو الجھانے کے لیے GhostBear کو فعال کرنا ضروری ہے، جس سے وہ عام HTTPS ٹریفک جیسا دکھائی دیتا ہے۔

B کیس اسٹڈی 2: غیر محفوظ عوامی ہاٹ اسپاٹس

استاد کا حل

گریڈنگ کی ہدایت

طلبہ کے جوابات میں درج ذیل نکات شامل ہونے چاہییں:

- منظرنامے کا تجزیہ: ایک انجینئر ہوائی اڈے کے کھلے Wi-Fi ہاٹ اسپاٹ سے جڑتا ہے اور اسے بار بار کنکشن منقطع ہونے کا سامنا ہوتا ہے۔
- تجویز کردہ حکمت عملی اور حل: VigilantBear تمام نیٹ ورک انٹرفیسز کو منجمد کر دیتا ہے، اور VPN ٹنل بحال ہونے تک غیر خفیہ شدہ ٹریفک لیکس کو بلاک کرتا ہے۔