نام: _____ تاریخ: _____ نمبر: _____

VPN کیسے سیٹ اپ کریں ورک شیٹ

Windows، macOS، Android، iOS، Linux اور راؤٹرز پر VPNs ترتیب دینا

VPN کا تعلیمی جائزہ

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 ورچوئل پرائیویٹ نیٹ ورکس (VPNs) کے بنیادی اصولوں سے متعارف کراتا ہے۔ آپ جائزہ لیں گے کہ خفیہ ٹنلز آپ کے ڈیٹا کو کیسے محفوظ بناتی ہیں، نیٹ ورک پروٹوکولز کیسے کام کرتے ہیں، اور رازداری کے لیکس کی نشاندہی اور تدارک کیسے کیا جائے۔

ورک شیٹ کے چیک پوائنٹس

- [ ] **حصہ 1-4: VPN کے تصورات اور پروٹوکولز 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 VPN گائیڈ کھولیں

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

آپ کا VPN لرننگ روڈ میپ

- تجارتی VPN ایپس کا مقامی کلائنٹس ترتیب دینے سے موازنہ کریں۔
- پورے گھر کے تحفظ کے لیے راؤٹرز پر VPN کنکشنز ترتیب دیں۔
- OVPN یا WireGuard کیز جیسی کنفیگریشن فائلیں ترتیب دیں اور ان کا انتظام کریں۔
- ٹنل ٹریفک کے لیے راؤٹر کے مخصوص پورٹس کھولیں اور محفوظ بنائیں۔
- DNS لیک چیکس اور کنکشن ٹیسٹس کے ذریعے کلائنٹ سیٹ اپس کی تصدیق کریں۔

ترتیب ورک شیٹ کی 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 VPN کلائنٹس کی ترتیب اور جانچ پر لاگو کریں۔ اور آخر میں اضافی سرگرمی "تیزی سے سوچیں"۔

VPN کنفیگریشن (تعارف)

VPN کو دستی طور پر سیٹ اپ کرنے سے آپ کو اپنی خفیہ کاری کیز اور نیٹ ورک روٹنگ پر مکمل کنٹرول ملتا ہے۔ چاہے آپ اپنے موبائل ڈیوائس پر مقامی کلائنٹ ترتیب دیں یا اپنے راؤٹر پر براہ راست VPN ٹنل نصب کریں، DNS لیکس کو روکنے اور تمام نیٹ ورک ٹریفک کو محفوظ بنانے کے لیے درست کنفیگریشن کلیدی ہے۔

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

چیک پوائنٹ 1: کثیر انتخابی چیلنج

1. موبائل ڈیوائسز پر VPN سیٹ اپ کرنے کا سب سے آسان طریقہ کیا ہے؟
   - A. ایپ اسٹور سے سرکاری VPN ایپ ڈاؤن لوڈ کرنا
   - B. آپریٹنگ سسٹم کی کرنل فائلوں کو دستی طور پر ایڈٹ کرنا
   - C. ڈیوائس ہارڈ ویئر پر کسٹم فرم ویئر فلیش کرنا
   - D. فون کو USB کے ذریعے ڈیسک ٹاپ کمپیوٹر سے جوڑنا

2. VPN کو براہِ راست اپنے راؤٹر پر انسٹال کرنے کا ایک فائدہ کیا ہے؟
   - A. یہ تمام مقامی ڈیوائسز کی کنکشن رفتار بڑھاتا ہے
   - B. یہ تمام منسلک نیٹ ورک ڈیوائسز کو خودکار طور پر محفوظ بنا دیتا ہے
   - C. یہ مقامی ISP کی سبسکرپشن فیس کی ضرورت کو ختم کر دیتا ہے
   - D. یہ ہارڈ ویئر راؤٹرز کی ضرورت کو مکمل طور پر ختم کر دیتا ہے

3. 'نیٹو' VPN کنفیگریشن سے کیا مراد ہے؟
   - A. آپریٹنگ سسٹم کی مقامی بلٹ اِن ترتیبات کے ذریعے کنکشن سیٹ اپ کرنا
   - B. VPN کو صرف اپنے آبائی شہر میں استعمال کرنا
   - C. صرف مقامی ملک کے سرورز سے جڑنا
   - D. اسمبلی زبان میں حسبِ ضرورت پروٹوکول لکھنا

4. دستی OpenVPN بیرونی کنفیگریشن کے لیے کیا درکار ہے؟
   - A. سرور کنکشن کے لیے حسبِ ضرورت لوگو ڈیزائن کرنا
   - B. سرٹیفکیٹ کیز پر مشتمل .ovpn پروفائل امپورٹ کرنا
   - C. گھر کے راؤٹر کا فزیکل مقام بدلنا
   - D. آپریٹنگ سسٹم فائر وال کو مکمل طور پر غیر فعال کرنا

5. ایک ایڈمنسٹریٹر سیٹ اپ میں اسپلٹ ٹنلنگ کیوں استعمال کرے گا؟
   - A. تمام انٹرنیٹ ٹریفک کو مکمل طور پر بلاک کرنا
   - B. مخصوص محفوظ ایپس کو محفوظ ٹنل بائی پاس کرنے کی اجازت دینے کے لیے
   - C. فزیکل روٹر کو دو الگ یونٹس میں تقسیم کرنے کے لیے
   - D. ایڈمنسٹریٹو مانیٹرنگ کے لیے خفیہ کاری غیر فعال کرنے کے لیے

چیک پوائنٹ 2: درست یا غلط چیلنج

6 سوال 6

6. راؤٹر VPN سیٹ اپ ایک آسان عمل ہے جس میں کسی تکنیکی مہارت کی ضرورت نہیں۔

درست غلط

7 سوال 7

7. Windows اور macOS میں IKEv2 اور L2TP کو سپورٹ کرنے والے نیٹو کلائنٹس موجود ہیں۔

درست غلط

8 سوال 8

8. WireGuard سیٹ اپ کرنے کے لیے پبلک اور پرائیویٹ کیز بنانا ضروری ہے۔

درست غلط

9 سوال 9

9. VPN ٹنل آپ کے مقامی نیٹ ورک پرنٹرز اور پرنٹ جابز کو محفوظ بناتی ہے۔

درست غلط

10 سوال 10

10. وہ اسمارٹ لاکس جو VPN ایپس نہیں چلا سکتے، انہیں کور کرنے کے لیے راؤٹر لیول VPN درکار ہوتا 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. گیٹ وے یعنی _____ کی سطح پر وی پی این لگانا اسمارٹ ٹی وی اور گیمنگ کنسولز کو تحفظ دیتا ہے۔
2. دستی OpenVPN کنفیگریشن کے لیے _____ سرور پروفائل درآمد کرنا ضروری ہے۔
3. بلٹ اِن او ایس کنفیگریشنز سسٹم کی _____ کلائنٹ سیٹنگز استعمال کرتی ہیں۔
4. WireGuard کی توثیق کرپٹوگرافک عوامی اور نجی _____ پر انحصار کرتی ہے۔
5. صارف دوست انسٹالیشن فراہم کنندہ کی سرکاری _____ کے ذریعے ممکن ہوتی ہے۔
6. کوئریز کو وی پی این _____ سرورز کے ذریعے بھیجنا نام کے حل کے ٹریکنگ لیکس سے بچاتا ہے۔

الفاظ کا بینک

ovpn. اسپلٹ ٹنلنگ ایپ ڈی این ایس راؤٹر کلیدی جوڑا لاگز نیٹو

اپنے جوابات یہاں لکھیں:

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

چیک پوائنٹ 4: نیٹ ورک تصورات کا ملان

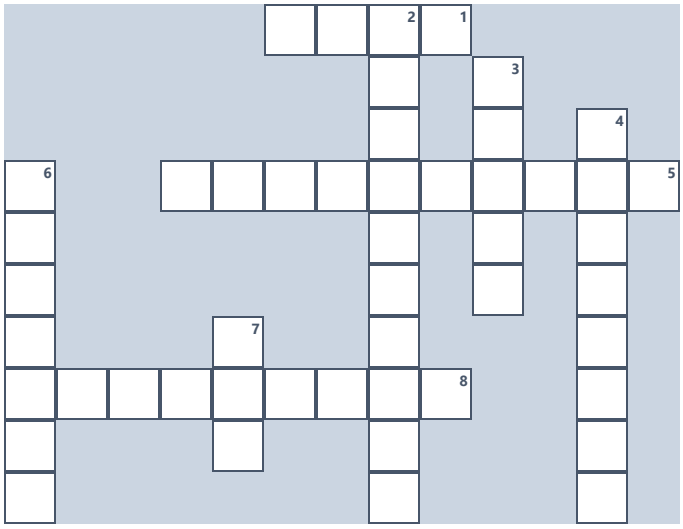
تعریفوں کا ملان

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. VPN ایپ		A — گیٹ وے کی سطح کی خفیہ کاری جو مقامی نیٹ ورک پر موجود تمام اسمارٹ آلات کو محفوظ بناتی ہے۔
2. راؤٹر VPN		B — سبسکرپشن سروس کی طرف سے فراہم کردہ سافٹ ویئر پیکیج جو آسان ایک کلک سیٹ اپ کے لیے ہوتا ہے۔
3. نیٹو کلائنٹ		C — ناکام سیٹ اپس کی خرابی دور کرنے کے لیے ایرر آؤٹ پٹس اور کلائنٹ اسٹیٹس لاگز کی جانچ کرنا۔
4. .ovpn پروفائل		D — ٹریفک کے راستوں میں فرق کرنا تاکہ مخصوص ایپس خفیہ ٹنل کو چھوڑ سکیں۔
5. کی جوڑی		E — ایپس نصب کیے بغیر آپریٹنگ سسٹم کی اپنی سیٹنگز کے اندر ٹریفک کو محفوظ بنانا۔
6. اسپلٹ ٹنلنگ		F — ڈومین لوک اپ لیکس روکنے کے لیے نیٹ ورک ریزولور ایڈریسز ترتیب دینا۔
7. DNS سرور سیٹ اپ		G — WireGuard ہینڈ شیکس قائم کرنے کے لیے درکار کرپٹوگرافک ٹوکنز (عوامی/نجی)۔
8. کنکشن لاگز		H — OpenVPN فائل فارمیٹ جس میں سرورز، پورٹ سیٹنگز اور سرٹیفکیٹ کیز ہوتی ہیں۔

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

1. ناکام سیٹ اپ کی خرابی دور کرنے کے لیے ایرر آؤٹ پٹ اور کلائنٹ اسٹیٹس ریکارڈز کی جانچ (4)

5. ایپس انسٹال کیے بغیر آپریٹنگ سسٹم کی اپنی سیٹنگز کے اندر ٹریفک کو محفوظ بنانا (10)

8. WireGuard ہینڈ شیک قائم کرنے کے لیے درکار کرپٹوگرافک ٹوکنز (عوامی/نجی) (9)

عمودی

2. ٹریفک کے راستے الگ کرنا تاکہ مخصوص ایپس انکرپٹڈ ٹنل کو بائی پاس کر سکیں (10)

3. گیٹ وے کی سطح کی انکرپشن جو مقامی نیٹ ورک پر تمام اسمارٹ آلات کو تحفظ دیتی ہے (5)

4. ڈومین لوک اپ لیکس روکنے کے لیے نیٹ ورک ریزولور ایڈریسز ترتیب دینا (8)

6. OpenVPN فائل فارمیٹ جس میں سرورز، پورٹ سیٹنگز اور سرٹیفکیٹ کیز شامل ہوتی ہیں (7)

7. سبسکرپشن سروس کی طرف سے فراہم کردہ سافٹ ویئر پیکیج جو ایک کلک سے آسان سیٹ اپ دیتا ہے (3)

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

1 افقی: ناکام سیٹ اپ کی خرابی دور کرنے کے لیے ایرر آؤٹ پٹ اور کلائنٹ اسٹیٹس ریکارڈز کی جانچ (4 حروف):

5 افقی: ایپس انسٹال کیے بغیر آپریٹنگ سسٹم کی اپنی سیٹنگز کے اندر ٹریفک کو محفوظ بنانا (10 حروف):

8 افقی: WireGuard ہینڈ شیک قائم کرنے کے لیے درکار کرپٹوگرافک ٹوکنز (عوامی/نجی) (9 حروف):

عمودی

2 عمودی: ٹریفک کے راستے الگ کرنا تاکہ مخصوص ایپس انکرپٹڈ ٹنل کو بائی پاس کر سکیں (10 حروف):

3 عمودی: گیٹ وے کی سطح کی انکرپشن جو مقامی نیٹ ورک پر تمام اسمارٹ آلات کو تحفظ دیتی ہے (5 حروف):

4 عمودی: ڈومین لوک اپ لیکس روکنے کے لیے نیٹ ورک ریزولور ایڈریسز ترتیب دینا (8 حروف):

6 عمودی: OpenVPN فائل فارمیٹ جس میں سرورز، پورٹ سیٹنگز اور سرٹیفکیٹ کیز شامل ہوتی ہیں (7 حروف):

7 عمودی: سبسکرپشن سروس کی طرف سے فراہم کردہ سافٹ ویئر پیکیج جو ایک کلک سے آسان سیٹ اپ دیتا ہے (3 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۔

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

الفاظ کی فہرست

ایپ، راوٹر، نیٹوکلائنٹ، پروفائل، کلیدیجوڑا، اسپلٹٹنلنگ، ڈیاینایس، لاگز

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. ایپ
B. راوٹر
C. نیٹوکلائنٹ
D. پروفائل
E. کلیدیجوڑا
F. اسپلٹٹنلنگ
G. ڈیاینایس
H. لاگز

تعریفیں اور ملان کے خانے	
1. ڈومین لوک اپ لیکس روکنے کے لیے نیٹ ورک ریزولور ایڈریسز ترتیب دینا۔	
2. ٹریفک کے راستے الگ کرنا تاکہ مخصوص ایپس انکرپٹڈ ٹنل کو بائی پاس کر سکیں۔	
3. گیٹ وے کی سطح کی انکرپشن جو مقامی نیٹ ورک پر تمام اسمارٹ آلات کو تحفظ دیتی ہے۔	
4. WireGuard ہینڈ شیک قائم کرنے کے لیے درکار کرپٹوگرافک ٹوکنز (عوامی/نجی)۔	
5. ایپس انسٹال کیے بغیر آپریٹنگ سسٹم کی اپنی سیٹنگز کے اندر ٹریفک کو محفوظ بنانا۔	
6. ناکام سیٹ اپ کی خرابی دور کرنے کے لیے ایرر آؤٹ پٹ اور کلائنٹ اسٹیٹس ریکارڈز کی جانچ۔	
7. OpenVPN فائل فارمیٹ جس میں سرورز، پورٹ سیٹنگز اور سرٹیفکیٹ کیز شامل ہوتی ہیں۔	
8. سبسکرپشن سروس کی طرف سے فراہم کردہ سافٹ ویئر پیکیج جو ایک کلک سے آسان سیٹ اپ دیتا ہے۔	

چیک پوائنٹ 7: الجھے الفاظ کا چیلنج

VPN کے اہم تصورات اور اصطلاحات ظاہر کرنے کے لیے نیچے دیے گئے حروف کو درست ترتیب میں لائیں۔ اپنے جوابات بھرے جانے والے ان پٹ باکسز میں لکھیں۔

1. ی پ ا _____

2. ن و ن ی ک ٹ ا ئ ل ٹ _____

3. ک ج ی ل و ا د ڑ ی _____

4. ی ی س ا ن ڈ ی ا _____

5. و ر ر ٹ ا _____

6. ئ و ا پ ف ل ر _____

7. س ل ا ن ٹ ل ن گ ٹ پ _____

8. ل ز گ ا _____

اضافی سرگرمی: تیزی سے سوچیں

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

1	سیٹ اپ مکمل ہونے کے بعد جانچنے کی چیزیں		
2	وہ ڈیوائسز جو VPN استعمال کر سکتی ہیں		
3	آپ کی جانی پہچانی VPN سروسز کے نام		
4	سفر کے دوران VPN استعمال کرنے کی وجوہات		
5	سیٹ اپ کے دوران لوگوں کی غلطیاں		
6	اس ورک شیٹ کے وہ الفاظ جو آپ یاد رکھنا چاہتے ہیں		
7	وہ سیٹنگز جو آپ سب سے پہلے آن کرتے ہیں		
8	وہ وعدے جو اچھا VPN فراہم کنندہ کرتا ہے		
9	VPN سیٹ اپ کرتے وقت کے مراحل		
10	وہ مقامات جہاں آپ VPN استعمال کریں گے		
11	جعلی Wi-Fi نیٹ ورک پہچاننے کے طریقے		
12	وہ چیزیں جو VPN چھپا سکتا ہے		
13	وہ چیزیں جو آپ کا انٹرنیٹ فراہم کنندہ دیکھ سکتا ہے		
14	مدد تلاش کرنے کے مقامات		
15	شروع کرنے کے لیے درکار چیزیں		

چیک پوائنٹ 8: VPN کیس اسٹڈیز

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

سارہ (کافی شاپ کی طالبہ)

👩‍💻 "ارے! میں Coffee & Bytes میں بیٹھا ہوں۔ یہاں 'Free_Wi-Fi_No_Password' نام کا غیر محفوظ عوامی نیٹ ورک ہے۔ میں اپنی اسکول کی ای میل میں لاگ اِن کرنا اور اپنی اسائنمنٹ اپ لوڈ کرنا چاہتا ہوں، لیکن مجھے ہیکرز کی فکر ہے۔ VPN کے بغیر اس نیٹ ورک کے استعمال کے کیا خطرات ہیں، اور VPN میرے ڈیٹا کو کیسے محفوظ بناتا ہے؟"

الیکس (مسافر طالب علم)

👩‍💻 "اوہ نہیں! میں ایک پروجیکٹ کے لیے بیرون ملک سفر کر رہا ہوں اور اپنے آبائی ملک کے ایک سرور پر ہوسٹ کی گئی بائیولوجی ڈاکومینٹری دیکھنے کی کوشش کر رہا ہوں۔ لیکن سائٹ کہتی ہے 'This video is not available in your current location.' مجھے کیوں بلاک کیا گیا ہے، اور VPN اسے دیکھنے میں میری کیسے مدد کر سکتا ہے؟"

چیک پوائنٹ 9: سائفر حل کریں

اپنی سرور کنفیگریشن کی تربیت مکمل کرنے کے لیے محفوظ ٹنلز ترتیب دینے کے بارے میں یہ چھپا ہوا 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	34		5	37	29		38	18		32	31	37	12		23	34	26	9	31

33	37	39	1	29	30

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 کے استعمال کے بارے میں ممکنہ صارفین کے سب سے عام سوالات اور جوابات کا جائزہ لیں۔

Q1: VPN کیا ہے اور یہ کیسے کام کرتا ہے؟

ورچوئل پرائیویٹ نیٹ ورک (VPN) آپ کے انٹرنیٹ کنکشن کو خفیہ کرتا ہے اور آپ کے ٹریفک کو محفوظ ریموٹ سرور کے ذریعے روٹ کرتا ہے۔ اس سے آپ کا عوامی IP ایڈریس چھپتا ہے اور VPN ٹنل سے گزرنے والے ٹریفک کے بارے میں مقامی نیٹ ورک کے مبصرین اور آپ کا ISP جو کچھ دیکھ سکتے ہیں وہ محدود ہو جاتا ہے۔

Q2: شروع کرنے کے لیے مجھے کیا چاہیے؟

آپ کو فعال VPN سبسکرپشن یا اپنا VPN سرور، ایک معاون آلہ، اور یا تو فراہم کنندہ کی ایپ یا دستی سیٹ اپ کی تفصیلات درکار ہیں: سرور ایڈریس، پروٹوکول اور آپ کی اسناد، کیز یا سرٹیفکیٹس۔ زیادہ تر لوگ بس سرکاری ایپ انسٹال کرتے ہیں، سائن ان کرتے ہیں اور کنیکٹ دباتے ہیں۔

Q3: میں ایپ کے بغیر Windows پر VPN کیسے سیٹ اپ کروں؟

Settings > Network & internet > VPN کھولیں، Add VPN منتخب کریں، اور پرووائیڈر کا سرور نام، VPN کی قسم (جیسے IKEv2 یا L2TP/IPsec) اور اپنی سائن اِن تفصیلات درج کریں۔ پھر Connect منتخب کریں۔

Q4: کیا VPN میری انٹرنیٹ کی رفتار کو سست کر دے گا؟

ہاں، تھوڑا سا۔ خفیہ کاری کا عمل اور VPN سرور تک فزیکل فاصلہ لیٹنسی اور اضافی بوجھ بڑھاتے ہیں۔ اثر فراہم کنندہ، پروٹوکول، سرور کے فاصلے، آلے اور نیٹ ورک کے حالات کے مطابق مختلف ہوتا ہے۔

Q5: میں macOS کیسے سیٹ اپ کروں؟

فراہم کنندہ کی macOS ایپ انسٹال کریں، یا System Settings > VPN کھولیں، VPN کنفیگریشن شامل کریں، IKEv2، L2TP over IPSec یا Cisco IPSec منتخب کریں، اور اپنے فراہم کنندہ کا سرور ایڈریس اور اسناد درج کریں۔

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

ورچوئل پرائیویٹ نیٹ ورکس کے استعمال کے بارے میں ممکنہ صارفین کے سب سے عام سوالات اور جوابات کا جائزہ لیں۔

Q6: کیا میں مفت VPN استعمال کر سکتا ہوں؟

مفت VPNs اشتہارات، محدود خصوصیات، استعمال کے تجزیات، ڈیٹا کی حدود یا آمدنی کے دیگر ماڈلز پر انحصار کر سکتے ہیں۔ صارفین کو استعمال سے پہلے فراہم کنندہ کی رازداری کی پالیسی، ملکیت، آڈٹس اور کاروباری ماڈل کا جائزہ لینا چاہیے۔

Q7: میں .ovpn فائل کیسے استعمال کروں؟

OpenVPN کلائنٹ انسٹال کریں، اپنے فراہم کنندہ یا ایڈمنسٹریٹر سے .ovpn پروفائل امپورٹ کریں، اور جڑیں۔ فائل میں سرور کا ایڈریس، پورٹ، UDP یا TCP کی ترتیب اور اکثر سرٹیفکیٹس اور کلیدیں ہوتی ہیں۔

Q8: میں بہترین VPN کا انتخاب کیسے کروں؟

آڈٹ شدہ نو لاگز پالیسیاں، مضبوط پروٹوکولز (WireGuard, OpenVPN)، محفوظ سرور مقامات، تیز رفتار، صرف RAM والے سرورز، کل سوئچ فیچر، اور انٹیلیجنس شیئرنگ اتحادوں (جیسے 5/9/14 آئیز) سے باہر دائرہ اختیار تلاش کریں۔

Q9: کیا میں اپنے فون اور اسمارٹ TV پر VPN استعمال کر سکتا ہوں؟

ہاں۔ جدید VPN فراہم کنندگان Linux، Windows، macOS، Android، iOS اور اسمارٹ TVs کے لیے مخصوص ایپس کے ساتھ ساتھ آپ کے گھریلو نیٹ ورک کے تمام آلات کے تحفظ کے لیے راؤٹر سیٹ اپ بھی پیش کرتے ہیں۔

Q10: کِل سوئچ کیا ہے؟

کل سوئچ ایک سیکیورٹی فیچر ہے جو VPN کنکشن ٹوٹنے پر آپ کی ڈیوائس کو خودکار طور پر انٹرنیٹ سے منقطع کر دیتا ہے۔ اس سے آپ کا غیر خفیہ ڈیٹا یا اصل IP ایڈریس لیک ہونے سے بچتا ہے۔

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

ورچوئل پرائیویٹ نیٹ ورکس اور محفوظ ٹنلنگ پروٹوکولز کے تکنیکی اور ساختی پہلوؤں کا جائزہ لیں۔

Q1: WireGuard، OpenVPN اور IKEv2 میں کیا فرق ہے؟

WireGuard ایک جدید، ہلکا پھلکا پروٹوکول ہے (صرف ~4,000 لائنوں کا کوڈ) جو تیز رفتار اور فوری کنکشن اوقات فراہم کرتا ہے۔ OpenVPN ایک انتہائی محفوظ، آزمودہ اوپن سورس پروٹوکول ہے۔ IKEv2 موبائل ڈیوائسز کے لیے بہترین ہے کیونکہ نیٹ ورک بدلتے وقت یہ جلدی دوبارہ کنیکٹ ہو سکتا ہے۔

Q2: میں WireGuard کو دستی طور پر کیسے سیٹ اپ کروں؟

wg genkey اور wg pubkey سے کلیدی جوڑا بنائیں، اپنی عوامی کلید سرور کے ساتھ شیئر کریں، اور ایسی کنفیگ لکھیں جس میں آپ کی نجی کلید، پیئر کی عوامی کلید، مجاز IPs اور اینڈ پوائنٹ درج ہوں۔ wg-quick ٹول اسے چالو کرتا ہے۔ [2]

Q3: WebRTC لیکنگ کیا ہے اور VPN اسے کیسے روکتا ہے؟

WebRTC ایک براؤزر پروٹوکول ہے جو VPN فعال ہونے کے باوجود آپ کے اصل مقامی اور عوامی IP ایڈریس ظاہر کر سکتا ہے۔ پریمیم VPNs اپنی ڈیسک ٹاپ/موبائل ایپس اور براؤزر ایکسٹینشنز میں WebRTC درخواستوں کو بلاک یا جعلی بنا دیتے ہیں۔

Q4: میں اپنے گھریلو راؤٹر پر VPN محفوظ طریقے سے کیسے سیٹ اپ کروں؟

جانچیں کہ آپ کا راؤٹر VPN کلائنٹ موڈ کو سپورٹ کرتا ہے، اس کے ایڈمن صفحے میں لاگ اِن کریں، اور فراہم کنندہ کی OpenVPN یا WireGuard فائل اپ لوڈ کریں۔ کچھ راؤٹرز کو پہلے فرم ویئر اپ ڈیٹ درکار ہوتی ہے؛ اس کے بعد نیٹ ورک کی ہر ڈیوائس ٹنل استعمال کرتی ہے۔

Q5: اوبفسکیشن VPN بلاکس کو کیسے بائی پاس کرتی ہے؟

اوبفسکیشن (یا "اسٹیلتھ VPN") VPN ٹریفک کو عام HTTPS ٹریفک (پورٹ 443) جیسا بنا دیتی ہے۔ اس سے حکومتوں یا اسکول/دفتر کے نیٹ ورکس کی طرف سے VPN روکنے کے لیے استعمال ہونے والی ڈیپ پیکٹ انسپیکشن (DPI) سے بچنے میں مدد مل سکتی ہے۔

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

ورچوئل پرائیویٹ نیٹ ورکس اور محفوظ ٹنلنگ پروٹوکولز کے تکنیکی اور ساختی پہلوؤں کا جائزہ لیں۔

Q6: اسپلٹ ٹنلنگ کیا ہے اور مجھے اسے کب استعمال کرنا چاہیے؟

اسپلٹ ٹنلنگ آپ کو منتخب کرنے دیتی ہے کہ کون سی ایپس خفیہ کردہ VPN ٹنل کے ذریعے روٹ ہوں اور کون سی براہ راست انٹرنیٹ سے جڑیں۔ اسے حساس بینکنگ ایپس کو VPN سے گزارنے کے لیے استعمال کریں جبکہ مقامی گیمز براہ راست جڑیں، تاکہ VPN سے شامل ہونے والی لیٹنسی سے بچا جا سکے۔

Q7: میں کیسے جانچ سکتا ہوں کہ میرا نیا VPN سیٹ اپ کام کر رہا ہے؟

جڑیں، پھر IP چیک کرنے والی سائٹ پر جائیں: اسے VPN سرور کا IP ایڈریس اور مقام دکھانا چاہیے۔ DNS اور WebRTC لیک ٹیسٹ چلائیں، اور کنکشن کو مختصر طور پر منقطع کر کے تصدیق کریں کہ کِل سوئچ ٹریفک کو بلاک کرتا ہے۔

Q8: اگر سیٹ اپ کے بعد میرا VPN نہ جڑے تو مجھے کیا چیک کرنا چاہیے؟

اپنا لاگ اِن یا کیز، سرور کا ایڈریس، اور یہ جانچیں کہ منتخب پورٹ اور پروٹوکول بلاک نہیں ہیں۔ UDP اور TCP کے درمیان یا کسی دوسرے سرور پر تبدیل کر کے دیکھیں، اور غلطیوں کے لیے ایپ کے کنکشن لاگز پڑھیں۔

Q9: DNS لیک سے تحفظ کیا ہے؟

DNS لیک پروٹیکشن آپ کی ڈیوائس کو مجبور کرتا ہے کہ ویب سائٹ لُک آپ کوئریز (DNS کوئریز) آپ کے ISP کے سرورز کے بجائے VPN کے نجی، خفیہ کردہ DNS سرورز کے ذریعے بھیجے۔ اس سے آپ کا ISP یہ نہیں دیکھ پاتا کہ آپ کون سی سائٹس دیکھتے ہیں۔

Q10: کیا VPN خود بخود شروع ہونا چاہیے؟

عموماً ہاں۔ زیادہ تر ایپس اسٹارٹ اپ پر چل کر خود بخود کنکٹ ہو سکتی ہیں، یا غیر محفوظ Wi-Fi پر، تاکہ دوسری ایپس کے ڈیٹا بھیجنا شروع کرنے سے پہلے آپ محفوظ ہوں۔

حصہ 11: 10 دلچسپ VPN حقائق اور عملی بصیرتیں

VPNs کی تاریخ، مارکیٹ اور ٹیکنالوجی کے بارے میں ان نہایت قیمتی، حقیقی دنیا کے حقائق اور بصیرتوں کا جائزہ لیں۔

1. نیٹو کلائنٹس

Windows اور macOS دونوں میں بلٹ اِن VPN کلائنٹس شامل ہیں جو IKEv2 اور L2TP/IPsec کو سپورٹ کرتے ہیں، اس لیے بہت سے کنکشنز اضافی ایپ کے بغیر ترتیب دیے جا سکتے ہیں۔

2. کی جنریشن

WireGuard کی فوری شروعات wg genkey سے پرائیویٹ کی بناتی ہے اور wg pubkey سے اس سے پبلک کی اخذ کرتی ہے۔ [2]

3. WireGuard انقلاب

WireGuard کا کوڈ بیس کارکردگی کے لیے انتہائی ہموار بنایا گیا ہے، جس سے روایتی پروٹوکولز کے مقابلے میں سیکیورٹی خامیوں کے لیے اس کا آڈٹ کرنا آسان ہوتا ہے۔ [1]

4. پروفائل فائلیں

.ovpn پروفائل سرور ایڈریس، پورٹ، پروٹوکول اور سرٹیفکیٹس کو یکجا کرتی ہے، اس لیے ایک ہی امپورٹ سے OpenVPN کنکشن سیٹ ہو جاتا ہے۔

5. ڈیفالٹ پورٹس

OpenVPN عموماً پورٹ 1194 استعمال کرتا ہے، جبکہ WireGuard کی سرکاری مثالیں UDP پورٹ 51820 استعمال کرتی ہیں؛ ٹنل کے جڑنے کے لیے فائر والز اور راؤٹرز پر ان پورٹس کی اجازت درکار ہو سکتی ہے۔

6. ڈیپ پیکٹ انسپیکشن

ڈیپ پیکٹ انسپیکشن (DPI) عام VPN پروٹوکولز کو پہچان کر بلاک کر سکتی ہے؛ TCP پورٹ 443 پر OpenVPN یا مبہم موڈ پر جانے سے مدد مل سکتی ہے۔

7. راؤٹر کا احاطہ

راؤٹر پر VPN اس کے پیچھے موجود ہر ڈیوائس کو محفوظ بناتا ہے، بشمول کنسولز اور اسمارٹ ٹی ویز جو VPN ایپ نہیں چلا سکتے، اور ہر ڈیوائس پر کچھ انسٹال کرنے کی ضرورت نہیں پڑتی۔

8. کیپ الائیو

NAT یا فائر وال کے پیچھے WireGuard کی PersistentKeepalive سیٹنگ، جو عموماً 25 سیکنڈ ہوتی ہے، ٹنل کو قابل رسائی رکھتی ہے۔ [2]

9. TUN/TAP ڈرائیورز

OpenVPN کو TUN/TAP ورچوئل نیٹ ورک انٹرفیس کے ساتھ کام کرنے کے لیے بنایا گیا ہے، جو زیادہ تر پلیٹ فارمز پر دستیاب ہے اور کلائنٹ انسٹال کرتے وقت سیٹ اپ ہو جاتا ہے۔ [3]

10. اسپلٹ ٹنلنگ

سیٹ اپ کے دوران اسپلٹ ٹنلنگ آپ کو منتخب ایپس یا ایڈریسز کو VPN سے خارج کرنے دیتی ہے، جو مقامی پرنٹرز یا ان ایپس کے لیے مددگار ہے جو VPN IP ایڈریسز بلاک کرتی ہیں۔

تکنیکی حوالہ جات اور ماخذ

اس ورک شیٹ میں استعمال ہونے والی حوالہ دی گئی اشاعتیں، کرپٹوگرافک وضاحتیں اور سرکاری دستاویزی معیارات۔

علمی اور صنعتی حوالہ جات

[1] WireGuard. (n.d.). WireGuard: fast, modern, secure VPN tunnel. https://www.wireguard.com/

[2] WireGuard. (n.d.). Quick Start. https://www.wireguard.com/quickstart/

[3] OpenVPN. (n.d.). OpenVPN 2.6 Manual. https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/

[4] NIST. (2020). SP 800-77 Rev. 1: Guide to IPsec VPNs. https://csrc.nist.gov/pubs/sp/800/77/r1/final

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

جوابی کلید: Windows، macOS، Android، iOS، Linux اور راؤٹرز پر VPN کی ترتیب

1 سوال 1

درست جواب: A

تدریسی نوٹ

موبائل ڈیوائسز پر VPN سیٹ اپ کرنے کا سب سے آسان طریقہ کیا ہے؟ → ایپ اسٹور سے سرکاری VPN ایپ ڈاؤن لوڈ کرنا

2 راؤٹر گیٹ وے سیٹ اپ لیٹنسی

درست جواب: B

تدریسی نوٹ

راؤٹر VPN گیٹ وے پر ٹریفک کو خفیہ کرتا ہے اور IoT ڈیوائسز، کنسولز اور اسمارٹ آلات کو محفوظ بناتا ہے جن میں مقامی VPN ایپلیکیشن انسٹال کرنے کی صلاحیت نہیں ہوتی۔ حوالہ: DD-WRT OpenVPN Clients، Linksys Router Config۔ [3]

3 سوال 3

درست جواب: A

تدریسی نوٹ

Windows اور macOS میں IKEv2 اور L2TP/IPsec جیسے پروٹوکولز کے لیے بلٹ ان کلائنٹس شامل ہیں، اس لیے اضافی سافٹ ویئر انسٹال کیے بغیر کنکشن سیٹ اپ کیا جا سکتا ہے۔

4 OpenVPN پروفائل امپورٹ روٹنگ کنٹرولز

درست جواب: B

تدریسی نوٹ

دستی کنفیگریشنز کے لیے .ovpn پروفائل کیز ڈاؤن لوڈ کرنا ضروری ہے جن میں ہدفی سرور پورٹس، پروٹوکول پیرامیٹرز (UDP/TCP) اور کرپٹوگرافک سرٹیفکیٹس ہوتے ہیں۔ حوالہ: DD-WRT OpenVPN Clients۔

5 اسپلٹ ٹنل روٹنگ رازداری

درست جواب: B

تدریسی نوٹ

اسپلٹ ٹنلنگ صارفین کو حساس کام کی ایپس کو خفیہ کردہ ٹنل کے ذریعے روٹ کرنے دیتی ہے جبکہ مقامی اسٹریمنگ یا گیمز VPN کے اضافی بوجھ کے بغیر براہ راست جڑ سکتے ہیں۔ حوالہ: IETF IKEv2 RFC۔

جوابی کلید: چیک پوائنٹ 2 – درست یا غلط

6 سوال 6

درست جواب: غلط

تدریسی نوٹ

راؤٹر سیٹ اپ کا مطلب ایڈمن پیج میں لاگ ان کرنا، VPN سپورٹ جانچنا اور کنفیگ فائلیں اپ لوڈ کرنا ہے۔

7 مقامی OS انضمام

رفتاریں

درست جواب: درست

تدریسی نوٹ

بڑے آپریٹنگ سسٹمز بغیر رکاوٹ سیکیورٹی کنکشن سیٹ اپ کو یقینی بنانے کے لیے پروٹوکول کا مقامی انضمام شامل کرتے ہیں۔ حوالہ: Microsoft Native Gateway، Apple Support Profiles۔

8 WireGuard کیز کی جوڑی بندی

اسنفنگ کا خطرہ

درست جواب: درست

تدریسی نوٹ

WireGuard پاس ورڈز یا CA چینز پر انحصار کرنے کے بجائے محفوظ P2P ہینڈ شیکس قائم کرنے کے لیے غیر ہم آہنگ کیز استعمال کرتا ہے۔ حوالہ: WireGuard CLI Specifications۔

9 مقامی ٹریفک بلاکس

فائر والز

درست جواب: غلط

تدریسی نوٹ

VPNs عموماً عوامی انٹرنیٹ ٹریفک روٹ کرتے ہیں، اور بعض اوقات مقامی نیٹ ورک پرنٹرز تک رسائی روک سکتے ہیں جب تک کہ دوسری طرح ترتیب نہ دیا جائے۔ حوالہ: Microsoft Native Gateway۔

10 سوال 10

درست جواب: درست

تدریسی نوٹ

وہ اسمارٹ لاکس جو VPN ایپس نہیں چلا سکتے، انہیں کور کرنے کے لیے راؤٹر لیول VPN درکار ہوتا 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 VPN ایپ	A .2 راؤٹر VPN	E .3 نیٹو کلائنٹ	H .4 .ovpn پروفائل
G .5 کی جوڑی	D .6 اسپلٹ ٹنلنگ	F .7 DNS سرور سیٹ اپ	C .8 کنکشن لاگز

چیک پوائنٹ 3: جوابی کلید – اہم اصطلاحات

1 راؤٹر	2 .ovpn	3 نیٹو	4 کلیدی جوڑا
5 ایپ	6 ڈی این ایس		

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

1 G – ڈیاینایس	2 F – اسپلٹٹنلنگ	3 B – راوٹر	4 E – کلیدیجوڑا
5 C – نیٹوکلائنٹ	6 H – لاگز	7 D – پروفائل	8 A – ایپ

اساتذہ کے لیے بحث کے نوٹس

اہم اصطلاحات:
یقینی بنائیں کہ طلبہ VPN ایپ، راؤٹر VPN اور نیٹو کلائنٹ 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۔

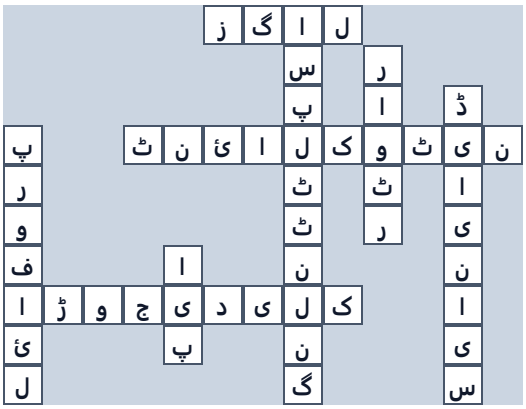
ماخذ کی جانچ:
طلبہ سے کہیں کہ ورک شیٹ کے ماخذ میں کم از کم ایک دعوے کی تصدیق کریں، اور اس پر بات کریں کہ اعداد و شمار، قیمتیں اور قواعد وقت کے ساتھ کیوں بدل سکتے ہیں۔

پہیلیوں کی کلیدیں اور استاد کے نوٹس

الفاظ کی تلاش کا حل

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

کراس ورڈ کا حل



کراس ورڈ حل کے لیے استاد کی گائیڈ

افقی

1 افقی: لاگز ناکام سیٹ اپ کی خرابی دور کرنے کے لیے ایرر آؤٹ پٹ اور کلائنٹ اسٹیٹس ریکارڈز کی جانچ (4 حروف)

5 افقی: نیٹوکلائنٹ ایپس انسٹال کیے بغیر آپریٹنگ سسٹم کی اپنی سیٹنگز کے اندر ٹریفک کو محفوظ بنانا (10 حروف)

8 افقی: کلیدیجوڑا WireGuard ہینڈ شیک قائم کرنے کے لیے درکار کرپٹوگرافک ٹوکنز (عوامی/نجی) (9 حروف)

عمودی

2 عمودی: اسپلٹٹنلنگ ٹریفک کے راستے الگ کرنا تاکہ مخصوص ایپس انکرپٹڈ ٹنل کو بائی پاس کر سکیں (10 حروف)

3 عمودی: راوٹر گیٹ وے کی سطح کی انکرپشن جو مقامی نیٹ ورک پر تمام اسمارٹ آلات کو تحفظ دیتی ہے (5 حروف)

4 عمودی: ڈیاینایس ڈومین لوک اپ لیکس روکنے کے لیے نیٹ ورک ریزولور ایڈریسز ترتیب دینا (8 حروف)

6 عمودی: پروفائل OpenVPN فائل فارمیٹ جس میں سرورز، پورٹ سیٹنگز اور سرٹیفکیٹ کیز شامل ہوتی ہیں (7 حروف)

7 عمودی: ایپ سبسکرپشن سروس کی طرف سے فراہم کردہ سافٹ ویئر پیکیج جو ایک کلک سے آسان سیٹ اپ دیتا ہے (3 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. پپا
2. نونیکٹائلٹ
3. کجیلوادڑی
4. پیسانڈیا
5. وررٹا
6. ٹواپفلر
7. سلانٹلنگٹپ
8. لزگا

ایپ
نیٹوکلائنٹ
کلیدیجوڑا
ڈیاینایس
راوٹر
پروفائل
اسپلٹٹنلنگ
لاگز

خفیہ سائفر چیلنج کی کلید

"محفوظ ڈیمن سے گیٹ وے لگائیں"

کیس اسٹڈیز کی جوابی کلید

A منظرنامہ A: عوامی نیٹ ورک کی سیکیورٹی

اسنفنگ اور خفیہ کاری | سارہ کی مشکل

گریڈنگ کی ہدایت

طلبہ کے جوابات میں درج ذیل نکات شامل ہونے چاہییں:

- خطرات: پیکٹ اسنفنگ، ڈیٹا کی مداخلت، اور مین ان دی مڈل حملے۔ اسی کافی شاپ کے نیٹ ورک پر موجود کوئی شخص اس کے لاگ اِن کی تفصیلات یا ہوم ورک فائل حاصل کر سکتا ہے۔
- VPN کا تحفظ: یہ نیٹ ورک پیکٹ پے لوڈز کو خفیہ کرتا ہے، جس سے VPN درست طور پر ترتیب دیے جانے کی صورت میں روکا گیا ٹنل ٹریفک غیر فعال مقامی نیٹ ورک جاسوسوں کے لیے ناقابلِ مطالعہ ہو جاتا ہے۔

B منظرنامہ B: بلاک شدہ وسائل تک رسائی

جیو بلاکنگ اور IPs | الیکس کی مشکل

گریڈنگ کی ہدایت

طلبہ کے جوابات میں درج ذیل نکات شامل ہونے چاہییں:

- بلاک ہونے کی وجہ: اسٹریمنگ ہوسٹ جیو بلاکنگ استعمال کرتا ہے، جو مسافر کے مقامی IP ایڈریس کو اس کے جسمانی ملک سے جوڑتی ہے اور علاقائی لائسنسنگ کی بنیاد پر اسے بلاک کر دیتی ہے۔
- VPN کیسے مدد کرتا ہے: ٹریفک کو اس کے آبائی ملک کے سرور سے گزار کر اس کا اصل مقام چھپانا۔ سائٹ کو آبائی ملک کا IP نظر آتا ہے، جس سے رسائی مل جاتی ہے۔